Fordham Urban Law Journal

Volume 8 | Number 4 Article 3

1980

Federal Legislative Proposals for the Protection of Privacy

Ludmila Kaniuga-Golad

FEDERAL LEGISLATIVE PROPOSALS FOR THE PROTECTION OF PRIVACY

I. Introduction

The right of privacy has been called a necessary ingredient of an ordered and free society.[1] Although not explicitly mentioned in the United States Constitution, a privacy interest is considered an underlying principle of the guarantees contained in the Bill of Rights.[2]

The courts and legislatures have established that a claim based on the invasion of one's right to privacy must arise under one of the four categories of the tort of invasion of privacy:[3] 1) unreasonable intrusion upon the seclusion of another;[4] 2) appropriation of a per-

---

1. Roe v. Wade, 410 U.S. 113, 153 (1973); *see* Doe v. Bolton, 410 U.S. 179 (1973); Eisenstadt v. Baird, 405 U.S. 438 (1972).

2. Soldiers may not be lodged in a private person's house without his consent. U.S. CONST. amend. III. Unreasonable searches and seizures are prohibited. *Id.* amend. IV. *See* Terry v. Ohio, 392 U.S. 1, 8-9 (1968); Katz v. United States, 389 U.S. 347 (1967); Boyd v. United States, 116 U.S. 616, 630 (1886). State action must operate within certain restrictions. U.S. CONST. amend. XIV, § 1. *See* Meyer v. Nebraska, 262 U.S. 390, 399 (1923). Most important, rights not expressly enumerated in the Constitution and its amendments are reserved to the people. U.S. CONST. amend. IX. *See* Griswold v. Connecticut, 381 U.S. 479, 486 (1965) (Goldberg, J., concurring). *See also* Galella v. Onassis, 487 F.2d 986, 995 n.12 (2d Cir. 1973); Palko v. Connecticut, 302 U.S. 319, 325 (1937); Note, *On Privacy: Constitutional Protection for Personal Liberty*, 48 N.Y.U.L. REV. 670 (1973); Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U.L. REV. 962, 1003 (1964); Yankwich, *The Right of Privacy; Its Development, Scope and Limitations*, 27 NOTRE DAME L. REV. 429 (1952).

The right of privacy has been called a "penumbra" from the Bill of Rights. Griswold v. Connecticut, 381 U.S. 479, 484 (1965). Recognition of the right of privacy is not recent. Ninety years ago, Warren and Brandeis wrote that the right of privacy is an evolving concept which finds its roots in the most basic common law protections of person and property. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) [hereinafter cited as Warren & Brandeis]. Throughout the common law, the individual has been granted the qualified right to determine, regardless of the medium or form of expression used, "to what extent his thoughts, sentiments, and emotions shall be communicated to others" by third parties. *Id.* at 198. Although absence of malice or truth of the matter are no defenses to the alleged violation of this right, once the subject consents to disclosure of the facts, his right is extinguished. *Id.* at 218.

3. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977); W. PROSSER, J. WADE & V. SCHWARTZ, CASES AND MATERIALS ON TORTS 1057-89 (6th ed. 1976); *See generally* Kalven, *Privacy in Tort Law - Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROB. 326 (1966); Davis, *What Do We Mean by "Right of Privacy?"*, 4 S.D. L. REV. 1 (1959).

4. *See* Froelich v. Adair, 213 Kan. 357, 516 P.2d 993 (1973) (where a wife, in attempting to prove that her husband was a homosexual, paid an orderly of a hospital, where her husband's alleged lover was undergoing an operation, to get samples of the lover's hair to be used in comparing it with that found in her husband's bed).

son's name or likeness;[5] 3) public disclosure of private facts which is highly offensive to a reasonable person not of legitimate concern to the public;[6] and 4) portrayal of an individual in a false light in the public eye.[7] So as not to leave a wrong remediless, it has been suggested that a new privacy action be recognized to protect an individual's privacy rights from the technological advances of the computer age.[8]

Computers have a virtually limitless capacity to store and retrieve information.[9] Presently, computers are readily available, compact and more cheaply able to store information than destroy it;[10] this has led to the expansion of governmental information practices.[11] Moreover, the information collected will frequently be

5. *See* Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68 (1905) (where an insurance company used Pavesich's picture together with a quote attributed to him to advertise insurance); Flake v. Greensboro News Co., 212 N.C. 780, 195 S.E. 55 (1938) (where a bakery used the photograph of a vaudeville actress to advertise bread without her consent).

6. *See* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975) (where a television station disclosed the name of the 17 year old victim of a rape. Although the court found that there was no tort since the name was a matter of public record, the opinion contains a good analysis of the requirements for the tort of public disclosure of private facts).

7. *See* Cantrell v. Forest City Publishing Co., 419 U.S. 245 (1974) (where a reporter inaccurately portrayed the family of an accident victim as living in abject poverty).

8. Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 GEO. L.J. 509, 532 (1969).

The problem presented by the diminution of the right of privacy as a result of "modern enterprise and invention" was itself anticipated almost a century ago. Warren & Brandeis, *supra* note 2, at 196. The power to control the flow of technologically transmitted information about his individuality comes from the individual's right of privacy. J.M. ROSENBERG, THE DEATH OF PRIVACY 143-61 (1969) [hereinafter cited as ROSENBERG].

9. One of the more advanced storage systems of International Business Machines, Inc. (IBM), the IBM 3850 Mass Storage System (MSS), provides for on-line storage of up to 472 billion bytes (characters) of data. This data is contained on cartridges measuring 2 inches in diameter by 4 inches in length. Each magnetic tape cartridge has a storage capacity of 50.4 million characters. IBM 3850 Mass Storage System (MSS) Introduction and Preinstallation Planning 2, 13 (GA. 32-0038-0, File number S370-07 (1st ed. Nov. 1978)).

10. A chip that has been developed by International Business Machines (IBM) has the calculating capabilities of the room size computer of twenty-five years ago yet is only one-quarter inch square. *The Computer Society*, TIME, Feb. 20, 1978, at 44. Developments such as this chip have led scientists to predict that the microelectronic revolution will "ease, enhance and simplify life in ways undreamed of even by the utopians. At home or office, routine chores will be performed with astonishing efficiency and speed." *Id.* at 46. The IBM chip has been mass produced to such an extent that computer systems can sell for as little as eight hundred dollars each and prices, it is promised, will go even lower. Paper will become obsolete and everything will be recorded through the processes of these chips. *Id.* at 46-47.

11. The power to collect information is inferred to be adjunct to the effective exercise of powers enumerated in the Constitution. *See* McGrain v. Daugherty, 273 U.S. 135, 160-75

inaccurate and potentially detrimental to the individual concerned.[12] Our legal system must strike a balance between the needs of a complex society for services and information and the possible dangers posed to the individual's recognized right of privacy by the availability of information maintained by the federal government.[13]

The difficulty inherent in this balancing process is demonstrated by the numerous extensive studies undertaken concerning this problem.[14] As a result of these studies, several bills are currently before both the House and Senate that attempt to resolve fairly the dilemmas posed.[15] Such bills include: Privacy of Research Records Act;[16] Federal Information and Privacy Board Act of 1978;[17] Omnibus Right to Privacy Act of 1979;[18] and Privacy Protection Amendments of 1979.[19]

Part II of this Comment will examine the failure of the proposal for a single data bank of federal information due to its inability to

---

(1927). *See also* Project, *Government Information and the Rights of Citizens*, 73 MICH. L. REV. 971, 1277-78 (1975). These powers include the power: (1) to enumerate the population, U.S. CONST. art. I, § 2, cl. 3; (2) to impeach, *id.* cl. 5; (3) to judge election returns, *id.* cl. 1; (4) to discipline and expel members of Congress, *id.* cl. 2; and (5) to legislate, *id.* § 1. The power to investigate, which is a necessary component of the power to legislate, has been limited to such investigation that pertains to the asserted legislative purpose, Sinclair v. United States, 279 U.S. 263 (1929), and which is expected to result in "valid legislations on the subject to which the inquiry referred." Kilbourn v. Thompson, 103 U.S. 168, 195 (1880).

12. In addition, such a widespread recording system seems to run counter to our criminal justice system, *i.e.*, rehabilitation is specious if the records will follow the subject always and mar any good faith efforts that he may attempt to make good. *See* DeWeese, *Reforming Our "Record Prisons": A Proposal for the Federal Regulation of Crime Data Banks*, 6 RUTGERS CAMDEN L.J. 26 (1974-75). *See also* Turner v. Reed, 22 Or. App. 177, 538 P.2d 373 (1975).

13. J. Rehnquist, in the first sentence of the Court's opinion in Chrysler Corp. v. Brown, 441 U.S. 281 (1979), delineated the problem thus: "The expanding range of federal regulatory activity and growth in the Government sector of the economy have increased federal agencies' demand for information about the activities of private individuals and corporations. These developments have paralleled a related concern about secrecy in Government and abuse of power." *Id.* at 285-86.

14. *See, e.g.*, SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE S. COMM. ON THE JUDICIARY, FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS, 93d Cong., 2d Sess. (1974) [hereinafter cited as SUBCOMMITTEE STUDY]; D. LINOWES, SURVEY RESEARCH LABORATORY OF THE UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, A RESEARCH SURVEY OF PRIVACY AND BIG BUSINESS (July 27, 1979) (on file with the Fordham Urban Law Journal) [hereinafter cited as LINOWES SURVEY]; U.S. DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY, NATIONAL INFORMATION POLICY (1976).

15. *See* note 14 *supra*.

16. S. 867, 96th Cong., 1st Sess. (1979) [hereinafter cited as S. 867].

17. H.R. 350, 96th Cong., 1st Sess. (1979) [hereinafter cited as H.R. 350].

18. H.R. 2465, 96th Cong., 1st Sess. (1979) [hereinafter cited as H.R. 2465].

19. H.R. 5559, 96th Cong., 1st Sess. (1979) [hereinafter cited as H.R. 5559].

safeguard privacy. Part III will synopsize the study of the Subcommittee on Constitutional Rights on the deficiencies in government data collection as it affects individual privacy rights. Part IV will examine the present privacy statutory scheme as established by the Freedom of Information Act[20] and the Privacy Act of 1974.[21] Part V will consider the already mentioned bills pending in Congress which purport to fill loopholes in the present law while balancing considerations of privacy and the public's need for information.[22]

II. The National Data Center as a Prior Legislative Alternative

In the mid-1960's, Congress considered a proposal for acquiring and centralizing the government's data on planning and research.[23] The main purpose of this proposal was to create a better, integrated information network for use by government, industry, and research communities. An agency to be called the National Data Center (NDC) was introduced as the central data bank. Statistical data obtained by a variety of federal agencies in the exercise of their statutory mandates was to be collected by the NDC. Presently, that information is maintained by separate agencies.

The NDC was to accumulate the data that is presently dispersed throughout a large number of different government agency files and maintain a current inventory of all data collected by federal agencies. By eliminating duplicative efforts of information collection and statistical analysis, the NDC would increase government efficiency. A public advisory committee consisting of representatives from various segments of the public, as well as interested government officials, would be formed. The committee's function would be to disclose publicly the bodies of data in the center, the persons using this data and their purposes. The committee also would be a clearinghouse for any prospective central data bank entries.[24]

---

20. 5 U.S.C. § 552 (1976).

21. *Id.* § 552(a) (1974).

22. *See* pt. V *infra.*

23. *The Computer and Invasion of Privacy: Hearings Before the Special Subcommittee on Invasion of Privacy of the House Committee on Government Operations,* 89th Cong., 2d Sess. (1966) [hereinafter cited as Ruggles Report].

24. *Invasions of Privacy: Hearings Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary,* 89th Cong., 2d Sess. (1966) [hereinafter cited as Dunn Critique].

Mechanical and electronic safeguards would be developed to forestall unauthorized access.[25] Files would be managed in such a way as to make it prohibitively expensive to obtain information about individuals by invading the Data Center. Stiff penalties would be levied for violation of any provision.

Proponents argued that it would be easier both to monitor disclosures from a centralized source and institute an improved system of safeguards.[26] In addition, because sensitive information collected by the Federal Bureau of Investigation and the Internal Revenue Service would not be contained in the NDC, the privacy invasions would be negligible.

The proposal, however, contained serious deficiencies. First, the information retained in the bank may be inaccurate or applied improperly.[27] There was also a potential for mistake in the transfer of information from agency files to the NDC. Second, it would be difficult to determine the existence of errors because of the bulk of information contained in the bank. Such misinformation could adversely affect an individual even though he is unaware of the cause of the difficulties.[28] Assuming the individual knew the cause, there would be little incentive to undertake a lawsuit because the proposal did not provide for damages.[29] Third, although proponents of

25. *See generally* Ruggles Report, *supra* note 23.

26. *See generally,* Dunn Critique, *supra* note 24. For a contrary view, *see* pt. III *infra.* (discussion of Subcommittee Study).

27. *Symposium: Computers, Data Banks, and Individual Privacy,* 53 MINN. L. REV. 211, 221-22 (1969) (transcript of speech given by John de J. Pemberton, Jr., Executive Director, ACLU, entitled *On the Dangers, Legal Aspects and Remedies*). For example, similar names may be confused and the records of one party applied to those of another improperly. A, not knowing why, is unable to get a mortgage. He finally discovers that information about B, a bad credit risk, having defaulted on previous payments, was mistakenly inserted into A's dossier due to the affinity of their names.

28. A survey conducted by the American Federal of Information Processing Societies (AFIPS) and Time magazine, administered in the spring of 1971, indicates that only 15 percent of the people responding to the survey claimed that they had some knowledge of how a computer system works. When asked about problems they had had because of a computer, the highest percentage of respondents, 34 percent, mentioned problems with billing. More than 90 percent of those surveyed believed that computers were being used for credit card billing, preparing bank statements and "compiling information files on U.S. citizens." NATIONAL ACADEMY OF SCIENCES, THE PROJECT ON COMPUTER DATABANKS OF THE COMPUTER SCIENCE & ENGINEERING BOARD, DATABANKS IN A FREE SOCIETY 481-85 (1972).

29. *See* Laird v. Tatum, 408 U.S. 1, 13-14 (1972). Here, the respondents claimed to represent a class whose rights were infringed by the existence of the Army's surveillance and data gathering system of lawful political activities. The Court held that failure on the part of the respondents to show concrete injury indicated the lack of a justiciable controversy and would bar the granting of relief.

the NDC claimed that only statistical records would be contained in the bank, the line between statistical and intelligence information is bound to become difficult to ascertain. In addition, trained intelligence personnel could derive potentially damaging data even from a statistical system.[30] Fifth, a computer breakdown in a central data bank would have potentially devastating consequences including an extremely damaging impact on the economy.[31] Finally, unauthorized access could result in a serious violation of privacy rights; indeed, the very nature of computer technology contributes to the uncertain status of safeguards against such access. People with remote terminals will potentially be able to misuse the information. Moreover, computer technology moves at such a rapid pace that safety considerations cannot be based on our present knowledge.[32] Making access difficult or expensive will not alleviate this problem. The art of electronic surveillance will only become more efficient, and once safeguards are penetrated, a violation of privacy interests is more serious because all the information is in one place.[33] Not to be overlooked is the significant damage government employees can inflict by negligence.[34]

---

30. ROSENBERG, *supra* note 8, at 35. It has also been alleged that such an all-encompassing system would encourage federal officials to engage in questionable surveillance tactics. The example used by the author was an optical scanner that reads mail and is hooked up to the NDC. Such a scanner could define the subject as one who associates with criminals simply because he sends a Christmas card once a year to a person of questionable character. *Id.* at 12.

31. *Id.* at 39.

32. Mr. Dennis Huaman of the General Electric Co., who is an internal security specialist with that company, feels that the most dangerous infringements are committed by persons knowledgeable in the computer field. "[M]ost of a company's data is actually taken when it is transmitted to other sites or transferred to hard copy . . . ." Scannell, *Security Expert Sees No Way to Stop D.P. Crime,* 13 Computerworld No. 50, at 7-8 (weekly ed. 1979).

33. For example, a systems programmer at a reasonable level of experience who gains access to a computer storage dump (a listing of the data which was in the Central Processing Unit at the time of a program error), will be able to decode various vital pieces of information about the programs and possibly systems security. Landon, *Software Putting Programmers Out of Business,* 13 Computerworld No. 50, at 22 (weekly ed. 1979).

34. Extreme care must be taken in selecting programming personnel. Currently, a bill is pending in Congress which would, by amending title 18 of the United States Code, make it a crime to use for fraudulent or other illegal purposes, a computer which is either owned or operated by the United States. This restriction would also apply to certain financial institutions and entities which affect interstate commerce. Federal Computer Systems Protection Act of 1979, S. 240, 96th Cong., 1st Sess. (1979) [hereinafter cited as S. 240]. *See also* Hamlin v. Kelly, 433 F. Supp. 180 (N.D. Ill. 1977), where the court held that because preserva-

The concept of a central data bank was first examined by the Committee on the Preservation of Economic Data.[35] This committee had been created by the Social Science Research Council[36] upon the recommendation of the American Economic Association.[37] After four years of study, the Committee submitted a report to the Council[38] which was referred for review to the Bureau of the Budget. The report recommended that: 1) the Bureau of the Budget, as the agency in charge of the Federal Statistical Program, take immediate steps to establish a Federal Data Center; 2) the Office of Statistical Standards of the Bureau of the Budget place an increased emphasis on the systematized preservation, in an accessible form, of important data prepared by those agencies engaged in statistical collection; and 3) the Social Science Research Council convene representatives from research institutions and universities to assist in developing an organization which could provide a clearinghouse for data requests made by individual scholars and federal agencies.[39] The Council report[40] maintained that any potential threat to privacy was outweighed by the public good served by centralized collection.[41]

This report caused much controversy. In 1968, a House Committee Report set forth its official response to the NDC concept.[42] It

---

tion of the individual's right is so overriding, inadequacy of staff or funds cannot be used as a defense by the agency.

35. SUBCOMMITTEE STUDY, *supra* note 14, at XVI.

36. *Id.*

37. *Id.*

38. Ruggles Report, *supra* note 23. The evaluation and study was conducted by Edgar S. Dunn of Resources for the Future, Inc.

39. *Id.*, app. 1, at 195.

40. *Id.*

41. Dunn Critique, *supra* note 24. The Task Force on the Storage of and Access to Government Statistics, in reaching the same conclusions as the Ruggles Report and the Dunn Critique, took as its focal point the organization and functioning of the NDC and recommended that Congress set standards of disclosure, such standards to be enforced by a Director of the Federal Statistical System. U.S. BUREAU OF THE BUDGET, REPORT OF THE TASK FORCE ON THE STORAGE OF AND ACCESS TO GOVERNMENT STATISTICS (1966). Further hearings were held in an attempt to balance the privacy issue against the efficiency of the computer. *Computer Privacy: Hearings Before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary*, 90th Cong., 1st Sess. (1967). While the NDC debate continued, the Joint Economic Committee issued a report which confirmed that current information did not meet the needs of the nation and advocated the NDC proposal. SUBCOMM. ON ECONOMIC STATISTICS OF THE JOINT ECONOMIC COMM., THE COORDINATION AND INTEGRATION OF GOVERNMENT STATISTICAL PROGRAMS, 90th Cong., 1st Sess. (1967).

42. HOUSE COMM. ON GOVERNMENT OPERATIONS, PRIVACY AND THE NATIONAL DATA BANK

concluded that the serious problems regarding the collection, use and security of personal information in a single information bank should delay implementation of the NDC until the technical feasibility of assuring privacy was fully explored.[43] The report argued that future plans include an independent supervisory commission to regulate not only the extent and operations of the NDC, but also the procedure by which information would be accessed.[44] As a result of this report, the NDC concept has not been revived.[45]

III. The Study of the Subcommittee on Constitutional Rights: Federal Data Banks and Privacy

A. Background

The use of computers for collecting data about citizens was explored by the Subcommittee on Constitutional Rights[46] in 1971.[47] The Committee began its work amidst the growing debate over the NDC. The study directly responded to five questions posed by Congress: 1) what personal information should be collected by the federal government;[48] 2) what means should be used to obtain it;[49] 3)

CONCEPT, H.R. Doc. No. 1842, 90th Cong., 2d Sess. (1968).

43. *Id.*

44. *Id.*

45. In fact, H.R. 2465, *supra* note 18, § 202(c), at 57 (*Title II: Privacy Act Amendments of 1979*), also rejects the development of a standard of universal personnel identifier, which entails the assigning of a number to each individual to identify him. This makes it easier to link together files of personal information which originally may have been obtained for different purposes. Davis, *A Technologist's View of Privacy and Security in Automated Information Systems*, 4 RUT. J. OF COMPUTERS & THE LAW 264, 273 (1974-76). *See* pt. II *infra*.

46. The subcommittee, which had been created at the beginning of the eighty-fourth Congress, has been interested in individual privacy since its inception and among its first actions were extensive hearings on wire tapping and government secrecy. After Senator Sam J. Ervin, Jr. became its chairman in 1961, the subcommittee began to concentrate on governmental infringement on individual privacy. Widespread studies of compartmentalized problems conducted by the subcommittee indicated that each was a part of a general schema of individual privacy juxtaposed against government's accumulation of information. As the computer became the obvious source of information activity, the subcommittee focused on an exploration of the privacy issue and mechanization. I SUBCOMMITTEE STUDY, *supra* note 14, at XXXIII - XXXIV.

47. *Federal Data Banks Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess., pt. I (1971).

48. *Id.* at XV.

49. *Id.*

who should have access to it;[50] 4) to what extent and under what conditions should information gathered for one purpose be made available for another;[51] and, 5) what rights do citizens have with respect to these data banks?[52]

B. Findings

The Subcommittee mailed surveys to fifty-four government agencies.[53] Although all of the agencies returned the survey, some left selected questions unanswered. The agencies polled by the Subcommittee indicated that they maintain 858 data banks[54] of varying size.[55] Over eighty-six percent of the reported data banks are computerized.[56] The study divides these data banks into three major types: 1) administrative, *i.e.*, those established to assist federal agencies in discharging their responsibilities to administer programs;[57] 2) evaluative, *i.e.*, those which collect information used to make certain status determinations regarding file subjects;[58] and, 3) statistical, *i.e.*, those which collect information about groups of subjects for management and planning purposes.[59] At least twenty-nine of the reported data banks appear to have been established to

---

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.* at XXXVII.

54. The author of the study feels that indications are that the agencies understate the scope of their personal data banks. *Id.* at XXXVII. The number of subjects contained in the data banks is impossible to state precisely; there are at least 1,245,699,494 records on individuals. *Id.* at XXXIX.

55. *E.g.*, The Air Force Special Weapons Center maintains a ten record manual security clearance file; the Department of Commerce Computerized Decennial Census data bank contains 204,000,000 records. *Id.*

56. *Id.* at XLIX, table 1.

57. Roughly sixty-nine percent of the data banks are administrative. *Id.* at L, table 2. E.g., the Small Business Administration's Accounting System, which is a data bank file containing information about the businesses which have applied for an S.B.A. loan: the name, address, race, type of business, bank used, annual sales, and credit rating. 6 *id.* at 3191.

58. The personnel security files of the Department of Defense, *e.g.*, which are compiled for security clearance purposes, contain various identifying data, including: physical descriptions, aliases, mental disorder, drug addiction, foreign travel, identification of foreign relatives and friends, neighborhood checks, sympathies with subversive organizations or any incidents in the individual's life which would involve a question of the individual's loyalty to his country. 2 *id.* at 1304.

59. E.g., The Decennial Census Data Bank of the Department of Commerce which compiles information across a broad spectrum of individuals as provided in 13 U.S.C. § 5 (1976).

collect derogatory information ("blacklists").[60] In addition, there exist numerous files containing potentially damaging information that are not maintained for the purpose of predicting specific criminal acts.[61] For example, one file compiled names of persons who were the subject of allegations which were later found to be unsubstantiated.[62]

The extent to which governmental information systems are authorized by explicit Congressional enactment varies from agency to agency. Eighty-four percent of the agencies surveyed were unable to cite explicit statutory authority; eighteen percent cited no statutory authority whatsoever.[63] The types of statutory authority which the agencies have for the collection of information fall into three categories: 1) express authority, where authorization flows from a definite statute;[64] 2) derivative, where authorization is considered essential to or necessarily required by specific programs which

60. The individuals contained in these files have been singled out for special treatment by federal agencies due to various "bad acts" on their part. 1 *id.* at XXXIX.

As an example of what these files contain, the "Debarred Bidder's List" is a list of contractors and grantees who are to be excluded from participation in Department of Housing and Urban Development programs for a period of time commensurate with the seriousness of the offense or inadequacy of performance. The offenses which lead to inclusion on this list include conviction of a criminal offense as an incident to attempting to obtain a public or private contract, violation of contract provisions, willful failure to perform terms of a contract, a record of failure to perform contracts, accepting a contingent fee in violation of the contractual provision against contingent fees, commission of fraud as an incident to carrying out or obtaining the contract. There are 802 subjects on this list. 3 *id.* at 2138-59. The Federal Communication Commission's blacklist consists of the name, address, date of birth of individuals, and a code number indicating the reason for their inclusion on the list, which includes: failure to pay a Commission forfeiture; license revocation; issuance of a bad check to the Commission; stopping payment on a check to the Commission; as well as information supplied by the FBI on persons who are allegedly subversive. The purpose of the list is to evaluate license applicants and grant licenses to only those persons who would serve the public interest. There are 12,000 subjects on this list. 5 *id.* at 2914-16.

61. *E.g.*, the Department of Justice Drug Enforcement Administration's Computerized Addict Files, which usually contain the name of the addict arrested, and enumerate which drugs were found in his possession at the time of arrest, the specific offense charged, etc. 4 *id.* at 2285.

62. The Defense Supply Agency's Security Files and Records, a computerized data bank, is such a file. 1 *id.* at XL.

63. One governmental unit unable to cite any statutory authority for keeping an information system was the White House. *Id.* table 3, & XLI.

64. A good example of a statutorily mandated data bank is the Department of Transportation's National Driver Register. *Id.* at XLI. The National Driver Register is a central clearing-house on driver licensing and is used to assist each state in locating the records that problem drivers may have established in other states. Its purpose is to keep irresponsible drivers off the roads. 4 *id.* at 2457-91.

themselves are derived from an express statutory mandate;[65] and, 3) implied, where authority is not absolutely necessary but thought to be useful in carrying out a program set up by specific legislation.[66]

Agencies receive information from three sources: 1) existing records;[67] 2) the subjects themselves;[68] and, 3) third parties.[69] Twenty-five percent of the agencies claimed reliance on all three sources.[70] A survey conducted at the University of Illinois by the former Chairman of the United States Privacy Protection Study Commission[71] revealed that private companies routinely disclose confidential personal data about their employees upon inquiry by a federal agency. Of the companies surveyed, forty-one percent responded that they had no policy as to which records were to be disclosed.[72] The nonexistence of a stringent policy as to disclosure of employee files leaves the person in charge, whether it be an executive or record clerk, with the discretion to determine what sensitive information a government agent will have access to, regardless of its relevancy to the agency's function or the particular agent's authorization. The Privacy Protection Commission has recommended to Congress "[t]hat an employer [be required to] articulate, communicate, and implement fair information practice policies which should include . . . limiting external disclosures of information in records kept on individual employees, former em-

65. Approximately twenty-one percent of the agencies responding claimed this type of legislative authority. *Id.* table 3. *E.g.*, National Defense Executive Reserve data bank of the Department of Commerce which is necessary to implement 5 U.S.C. 301 (1976). *Id.* at 242.

66. Forty-five percent of agencies surveyed cite this authority. SUBCOMMITTEE STUDY, *supra* note 14, table 3. *E.g.*, the Office of Economic Opportunity cites the agency's broad legislative mandate to "evaluate poverty" as authority for ten of its data banks. *Id.* at XLI.

67. *I.e.*, data banks which derive their contents from other data banks. Seventy-one percent of the 469 agencies responding to this question stated that they rely on existing data banks, *e.g.*, the Department of the Army. *Id.* table 9.

68. Sixty-four percent of the agencies responding utilize subject-provided information, *e.g.*, the Internal Revenue Service; the Decennial Census; Selective Service System. *Id.* table 9. One necessarily queries whether the individual really is providing this information voluntarily since these agencies compel disclosure on pain of criminal penalties.

69. Forty-one percent of the agencies rely on the third party sources. *E.g.*, security clearance and background check files. *Id.* at XLVIII & table 9.

70. Twenty-five percent of the agencies rely on all three sources. *E.g.*, Department of the Air Force; Department of Health, Education, and Welfare; Veterans Administration. *Id.* table 9.

71. LINOWES SURVEY, *supra* note 14, at 7.

72. *Id.*

ployees, and applicants . . . ."[73]

A large portion of the data banks are kept without the individual's knowledge. Forty-two percent of the 469 agencies responding stated that subject individuals are not notified of their inclusion in a data bank.[74] Virtually all of the intelligence files fall into this category.[75] Twenty-seven percent of the agencies responding said that subjects should realize that data on them is kept by the agency from their dealings with a particular agency.[76] The Selective Service Administration explained that because the individual subjects provide it with information, they should infer that it will be placed in a data bank.[77] Only thirty percent of the agencies expressly inform subjects that the data they supply will be placed in a bank.[78]

The damages which may potentially result from a breach of an individual's privacy rights may be eliminated by granting a subject the right to review his file. Fifty-three percent of the agencies responding to a question on this issue stated that subjects are allowed to review their entire files.[79] However, because so few individuals are aware of their inclusion in a file, a right of review is, at best, illusory. Approximately thirty-three percent of the agencies affirmed that subjects are not allowed to review their own files at all.[80] Other agencies responded that individuals are afforded review

---

73. *Id.* at 9.

74. *E.g.*, Department of Justice Internal Security Division; the White House Talent Bank; the Commerce Department's Executive Reserve. SUBCOMMITTEE STUDY, *supra* note 14, table 4.

75. *Id.*

76. *E.g.*, The Veterans Administration said that subjects should infer that they are placed in a data bank from the computerized benefit checks they receive. *Id.* at XLII & table 4.

77. 6 *id.* at 3132. Governmental units frequently use this "consent and waiver" defense, whereby the subject implicitly consents to disclosure of the information once it is released to the government. Such a defense was approved in Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975), where the United States Supreme Court held that once information is contained in official records, disclosure thereof is permissible. *Id.* at 492.

78. The Internal Revenue Service includes a note about the computerized master file on Income Tax forms. 5 SUBCOMMITTEE STUDY, *supra* note 14, at 2630. The Securities and Exchange Commission notifies by press release. 6 *id.* at 3088.

79. 1 *id.* at XLIII. The Marines provide subjects with a printout of their individual file at least once a year. 2 *id.* at 1251.

80. 1 *id.* at XLIII. Such is the case for most of the intelligence data banks. *E.g.*, Department of Justice's Organized Crime Information System. 4 *id.*; Drug Enforcement Administration Addict Files. *Id.* at 2198.

within the ambits of the Freedom of Information Act.[81] Fourteen percent of the agencies stated that they allow subjects to review only selected data.[82] Only the Air National Guard *requires* personnel to review their files once a year.[83]

Although individual subject access is considerably limited, the information contained in each federal agency data bank is readily passed on to other federal, state and local agencies pursuant to regular operating procedures.[84] Sixty percent of the agencies grant other federal agencies some degree of access.[85] Twenty-five percent allow direct access either by routine distribution of data or computer interface.[86] The Internal Revenue Service, for example, which vows confidentiality, does distribute some information to various government agencies.[87] Law enforcement agencies generally permit other agencies direct automated access by computer interface. Nineteen percent grant other agencies access to the files upon request.[88] Twelve percent allow access according to certain established agency procedures.[89] Many allow disclosure to other agencies as members of the general public under the FOIA.[90] Three percent of the agencies responding consider the file data to be public information.[91]

---

81. 5 U.S.C. § 552 (1976). For a discussion of the Freedom of Information Act, *see* pt. III(A) *infra*.

82. This is true for most agencies' personnel files. 1 SUBCOMMITTEE STUDY, *supra* note 14, at XLIII.

83. 2 *id.* at 318.

84. 1 *id.* at XLIV & table 6.

85. *Id.* The Defense Supply Agency's Control Index File of security clearances is maintained for the benefit of "user agencies." *Id.* at XLIII.

86. *Id.* at XLIV. Interface is defined as: "A shared boundary; e.g., the boundary between two systems, or between a computer and one of its peripheral devices." G. DAVIS, COMPUTER DATA PROCESSING 636 (2d ed. 1973).

87. 1 SUBCOMMITTEE STUDY, *supra* note 14, at XLIII. Although agencies other than the IRS are not permitted direct access to the Master Files, the specific information they request is extracted and provided to them by the Service. States have direct access to magnetic tapes of tax return information. 5 *id.* at 2630.

88. *Id.* at XLIV. *E.g.*, The Commodity Exchange Authority of the Department of Agriculture operates its data banks under an express Congressional mandate requiring that its findings be made available to other agencies upon request. 1 *id.* at 180.

89. *Id.* at XLIV. One agency using such procedures is the Department of the Army. *Id.* table 6.

90. *Id.* at XLIV. *E.g.*, the Appalachian Regional Commission. "Project data is public information and governed by the Freedom of Information Act." *Id.* at 100. Most of the data consists of economic information relating to the Appalachian Region, *e.g.*, employment statistics.

91. *Id.* at XLV. *E.g.*, The U.S. Coast Guard permits public access to the Boating Regis-

The security precautions utilized by the agencies differ.[92] Of the 471 agencies responding to the security inquiry, ninety-five percent acknowledged that some level of precaution is taken to secure the data from unauthorized access;[93] hence, five percent of the agencies admitted to engaging in no security arrangements whatsoever.[94] The most common security arrangement utilized by the agencies is physical security.[95] The systems vary from the very tight security used for the White House Central files, which are electronically coded and kept in locked, restricted access vaults under constant Secret Service surveillance,[96] to the shockingly lax security used for the Federal Deposit Insurance Corporation files,[97] which are kept only in ordinary locked file cabinets.[98] Twenty-six percent of the agencies claim that only a few people have the knowledge required to access the data file and fifteen percent claimed that these systems are electronically safeguarded by highly sophisticated computerized codes.[99] One agency uses the most secure measure: destruction of the data when the purpose for which it was originally collected is achieved.[100]

Two deficiencies emerge from these studies: the lack of statutory authorization for both the gathering of sensitive information and its subsequent compilation into data banks and the lack of ade-

---

tration and Motorboat Accident systems and allows relatives of subjects to see parts of the Merchant Seaman Locator File. *Id.*

92. *Id.* table 8.

93. *Id.*

94. *Id. E.g.*, Army statistical and administrative data banks. In response to the question regarding security precautions for its highly sensitive Narcotic Offender File, which was established to collect information as it relates to drug offenders within the U.S. Army and which contains the name of the offender and the type of offense within the file, the subcommittee received a "not applicable." 2 *id.* at 1176-77.

95. 1 *id.* table 8. The most common physical security methods are guarded entry, locked files, etc. *Id. See* note 101 *infra.*

96. SUBCOMMITTEE STUDY, *supra* note 14, at LVII & table 8.

97. 5 *id.* at 2929-48. These files contain vast amounts of potentially derogatory information, *e.g.*, financial reports of individuals who have dealings with member banks. *Id.*

98. *Id.* at 2930. The Air Force Aeronautical Chart and Information Center Upward Mobility File is "kept secure in the career development counselor's desk." 2 *id.* at 307.

99. 1 *id.* at XLVII. These special codes are part of the system's software. *E.g.*, the Department of Agriculture has a proposed data bank which will screen all requests for information.

100. This is the practice of the Department of Defense, Installations and Logistics Branch's Housing Referral Office data bank. 2 *id.* at 1341. The author of this study suggests that if this practice were followed by other agencies there would be less need for developing expensive and expansive means of security. 1 *id.* at XLVII.

quate security measures within the majority of the agencies surveyed.[101]

IV. The Present Legislative Scheme: the Freedom of Information Act and the Privacy Act of 1974

Present government information policy is regulated by the Freedom of Information Act[102] and the Privacy Act of 1974.[103] Their interaction is complex because the FOIA is generally viewed as a disclosure statute while the Privacy Act mandates nondisclosure. Under the FOIA, government-held information must be disclosed to any requesting individual unless the data falls into one of the nine FOIA exemptions, in which case the decision to disclose falls entirely within the discretion of the agency holding the information.[104] The Privacy Act's Conditions of Disclosure section[105] reflects Congressional response to the potential for abuse of disclosure with respect to the release of personal information and it is in this area that the greatest conflict between the two statutes occurs. Subsection (b)(2) of the Privacy Act exempts materials the FOIA requires to be disclosed from the general Privacy Act requirement that written consent from the subject individual be obtained prior to disclosure to third parties of information about the individual kept by

101. The Department of Investigation of the City of New York in its Guidelines for Computer Security recommends that computer facilities be kept secure (1) physically: via structural barriers; absence of windows in the computer equipment rooms; metal-covered doors with hinges on the inside; any windows are to be alarmed; closed circuit television monitoring; twenty-four hour guards; restriction of visitor access to preclude forced entry; location of the room in an area where exposure to traffic is minimal; (2) electronically: access restricted to designated individuals who require access in the performance of their official duties; logical access to the data files and software protected by appropriate systems software, password, and encryption algorithms; access control of remote terminals, and minimization of the use of the acoustic coupler, which is very insecure; (3) by risk management procedures: each agency head is to evaluate sensitivity of the data and must assume that hostile agents are prepared to take full advantage of significant system vulnerabilities. If the risk is too high, top management may determine that automated support is unwarranted. Protection should be commensurate with sensitivity. Department of Investigation of the City of New York, Guidelines for Computer Security, (Systems Security Standard #GCS-1, prepared by Rolf Moulton, issued on Mar. 1, 1979).

102. 5 U.S.C. § 552 (1976).

103. *Id.* § 552a.

104. *See* note 111 *infra.*

105. 5 U.S.C. § 552a(b) (1976). The Ninth Circuit Court of Appeals recently ruled that "the FOIA applies to computer tapes to the same extent it applies to any other documents." Rosenberg, *Computer Files Found Not Exempt From FOIA,* 13 Computerworld No. 49, at 16 (weekly ed. 1979).

the agency. Thus, the most important issue in most disclosure disputes is whether the requested information falls within the FOIA disclosure requirements. In practice, the result has been that such information, which falls within one of the nine exemptions of the FOIA and thus not required to be disclosed, will be withheld from the requesting individual. Conversely, as courts interpret the FOIA disclosure mandates more broadly, less material can be regulated by the Privacy Act.

A. The Freedom of Information Act (FOIA)

Many of the agencies surveyed by the Subcommittee on Constitutional Rights[106] cited the FOIA as their guideline for allowing individuals the opportunity to review their own files. The Freedom of Information Act regulates the disclosure of government-held data. Its mandate to disclose information to individuals reflects the same concerns raised by the Subcommittee on Constitutional Rights.[107] Under the FOIA, an individual is allowed access to agency opinions, policy statements, and agency manuals and instructions that affect the public interest.[108] An agency that refuses to allow any individual access to such information forfeits its right to use the material against the individual.[109] The FOIA allows an agency to delete from the information granted to a requesting party names of private individuals if disclosure thereof would constitute an excessive invasion of the subject's privacy.[110] Unless the information falls within one of the nine FOIA exemptions from the disclosure rule,[111] third parties are frequently granted access too readily because the ultimate decision of whether to disclose information is left up to the

106. *See* pt. III *supra*.

107. *Id.*

108. 5 U.S.C. § 552(a)(2)(A)-(C) (1976).

109. *Id.* § 552(a)(1)-(2).

110. *Id.* § 552(a)(2).

111. Briefly, the exemptions are: (1) Matters which are properly classified as secret in the interest of national defense or foreign policy by an executive order; (2) Information that is related exclusively to an agency's internal personnel rules; (3) Matters which are exempted from disclosure by a statute other than FOIA; (4) Trade secrets and confidential commercial or financial information; (5) Inter- or intra- agency memoranda not available by law to another party; (6) Files, such as personnel or medical files, which constitute an unwarranted invasion of privacy; (7) Investigatory records compiled for law enforcement purposes; (8) Information gathered by an agency responsible for the regulation or supervision of financial institutions; and (9) Geological or geographical information concerning wells. 5 U.S.C. § 552(b)(1)-(9) (1976).

agency itself.[112] The FOIA further provides that if certain information is subject to an exemption, the exempted data should be segregated from the body of the record, the remainder to be released to the individual seeking the data.[113] An individual may challenge an agency's refusal to release data in the United States District Court. The FOIA grants the court the power to order record production.[114] Courts will arrive at a decision by balancing the privacy of the individual who is the topic of the data and the public's right to know the information.[115] Generally, if the person seeking disclosure is the subject of the data, access will be more readily granted than would be if he were a member of the general public because in the former situation there may not be an invasion of the individual's privacy.[116]

The FOIA disallows the subject of the record certain access thereto, although revelation would be crucial to his privacy interests. Especially troublesome in this area are exemptions one,[117] four,[118] six,[119] and seven.[120] Exemption one permits denial of access if the data is determined to be essential to national security.[121] The President may, in his discretion, establish that an item is one of national security and thus eliminate it from the public domain. The fourth exemption exempts trade secrets and commercial information from disclosure where such information was given with the

112. Congress, however, cannot be denied any data, private or otherwise. *Id.* § 552(c) (1976).

113. "Any reasonable segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection." *Id.* § 552(b).

114. *Id.* § 552(a)(4)(B).

115. Thus, newsmen frequently have brought suit to compel disclosure of information in their capacity as information-bearers to the public. *E.g.*, Nixon v. Sampson, 389 F. Supp. 107 (D.D.C. 1975); Philadelphia Newspapers, Inc. v. HUD, 343 F. Supp. 1176 (E.D. Pa. 1972).

116. *See* Black v. Sheraton Corp. of Am., 371 F. Supp. 97 (D.D.C. 1974). Here, a subject of an F.B.I. investigation was granted access to his file because it did not involve a law enforcement proceeding and the file had been closed for quite a while prior to suit.

117. 5 U.S.C. § 552(b)(1) (1976). *I.e.*, national security data. *See* note 111 *supra.*

118. 5 U.S.C. § 552(b)(4) (1976). *I.e.*, trade secrets and confidential commercial or financial information. *See* note 111 *supra.*

119. 5 U.S.C. § 552(b)(6) (1976). *I.e.*, personnel, medical, or other intimate files. *See* note 111 *supra.*

120. 5 U.S.C. § 552(b)(7) (1976). *I.e.*, investigatory law enforcement records. *See* note 111 *supra.*

121. *See* Environmental Protection Agency v. Mink, 410 U.S. 73 (1973).

expectation of confidentiality.[122] Under the sixth exemption, the disclosure of personnel, medical, and other files, which would constitute an unwarranted invasion of individual privacy, is prohibited.[123] Finally, the seventh exemption requires that law enforcement files be kept secret if disclosure thereof would interfere with the criminal process or deprive a defendant of a constitutional right.[124]

The sixth and seventh exemptions are most likely to affect an individual by prohibiting disclosure of information which is clearly sensitive and potentially erosive of individual privacy.[125] The most frequent argument made against these two exemptions is that the public may have a genuine interest in the data. An equitable solution to this conflict is the one subscribed to by the United States Supreme Court in *Department of the Air Force v. Rose,*[126] wherein the Court ordered disclosure of the information about military honor codes only after identification of individual subjects was removed.[127] This ruling did not impair the value of the data because identification of the individuals in the file was immaterial to the interested public.

B. The Privacy Act of 1974

In 1974, Congress passed an amendment to the FOIA,[128] popularly known as the Privacy Act of 1974 (the Act),[129] to restrict the ease of disclosure to third parties inherent under the FOIA.[130] The

122. *See* Getman v. NLRB, 450 F.2d 670 (D.C. Cir.), *appeal for stay denied,* 404 U.S. 1204 (1971); Stone v. Export-Import Bank of the United States, 552 F.2d 132 (5th Cir.), *rehearing en banc denied,* 555 F.2d 1391 (5th Cir. 1977), *cert. denied,* 434 U.S. 1012 (1978). In *Stone,* the court denied disclosure of the terms of a loan made to a Soviet bank, reading the statute as stating that the bank was a "person" expecting confidentiality of a trade secret.

123. *See* Robles v. EPA, 484 F.2d 843 (4th Cir. 1973).

124. *See* National Public Radio v. Bell, 431 F. Supp. 509 (D.D.C. 1977).

125. *See* Comment, *Freedom of Information Act: the Expansion of Exemption Six,* 27 U. FLA. L. REV. 848 (1975).

126. 425 U.S. 352 (1976).

127. *Id.* at 380.

128. *See* pt. IV(A) *supra.*

129. Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (1976)). The note accompanying the Privacy Act explains that the need for specific legislation to safeguard a "personal and fundamental right protected by the Constitution of the United States" is a reaction to the increasing use of sophisticated technology in collecting and disseminating information for the Government. *Id.*

130. *See* text accompanying notes 117-27 *supra.*

Act also attempts to ease an individual's access to records kept about him. Subject individuals are able, under this Act, to gain access to information still maintained in secrecy pursuant to one of the exemptions of the FOIA.[131] The Act provides the subject of the data some control over the information that has been collected about him.[132] The subject may: 1) determine what records are collected;[133] 2) have access to the records and correct discrepancies;[134] and 3) prevent nonconsensual transferral of the information amongst agencies or other individuals.[135] An individual must be given a copy of his record upon request from the agency that maintains the data.[136] Upon receipt of such copy, the subject has the right to request that the information collection agency correct or

---

131. *See* note 111 *supra.*

132. Congress stated its findings as follows:

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States.

Privacy Act of 1974, Pub. L. No. 93-579, § 2(a), 88 Stat. 1896.

133. This is effected by the requirement that:

Each agency, with respect to each system of records under its control, shall -

(1) . . . keep an accurate accounting of —

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section [criminal law enforcement activity], make the accounting . . . available to the individual named in the record at his request;

5 U.S.C. § 552a(c) (1976).

134. *Id.* § 552a(d).

135. *Id.* § 552a(b).

136. The Act states:

"[U]pon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, [the agency shall] permit him . . . to review the record and have a copy made of all or any portion thereof in a form comprehensible to him . . . ." *Id.* § 552(d)(1).

amend any portion of the record which is inaccurate, incomplete, irrelevant or untimely.[137] The subject is entitled to administrative review[138] should the agency deny such a request and to judicial review in the district court.[139] The district court is given jurisdiction to hear suits brought under the Privacy Act if: 1) a request to amend has been denied by the reviewing officer;[140] 2) administrative review of refusal to amend has been denied;[141] 3) requests to access the records have been denied;[142] 4) an inaccurate, untimely, irrelevant, or incomplete record has led to an adverse determination as regards the subject individual;[143] and 5) an individual has been adversely affected by any other failure to comply with the Act.[144] The court has the power to inspect the records *in camera* to determine whether the information has been withheld unjustifiably and, in its discretion, to order the agency to amend the record.[145]

Prior to disclosure of an individual's record to a third party,[146] the disclosing agency must obtain the individual's consent[147] and

137. *Id.* § 552a(d)(2)(b)(i).

138. Such administrative review is to be accorded the subject within thirty working days. If amendment is still refused, the subject has the right to file a statement of reasons for amendment which must be included with every disclosure of the record. *Id.* § 552a(d)(3).

139. *Id.* § 552a(g)(1). The courts, though, are often reluctant to curb disclosure of information which they feel is legitimately necessary to either another agency or to the public interest. Thus, in Jaffess v. HEW, 393 F. Supp. 626 (S.D.N.Y. 1975), the court felt that "[t]he present thrust of decisional law does not include within its compass the right of an individual to prevent disclosure by one governmental agency to another of matters obtained in the course of transmitting the agency's regular functions." *Id.* at 629. In Tennessean Newspapers, Inc. v. Levi, 403 F. Supp. 1318 (M.D. Tenn. 1975), the court granted the local press access to information about arrests and indictments from the United States Attorney's office, asserting that there exists a legitimate public interest in discovering the identity of criminal suspects.

140. 5 U.S.C. § 552a(g)(1)(A).

141. *Id.*

142. *Id.* § 552a(g)(1)(B).

143. *Id.* § 552a(g)(1)(C).

144. *Id.* § 552a(g)(1)(D).

145. *Id.* § 552a(g)(3)(A). Thus, in Mervin v. Bonfanti, 410 F. Supp. 1205 (D.D.C. 1976), the court decided to conduct an *in camera* evaluation of the records the plaintiff was seeking to inspect since the dossier contained evaluations of plaintiff which had been submitted to the government in connection with plaintiff's application for a position with the Social Security Administration. The judge noted that the *in camera* evaluation was necessary in order to make it simpler for the court to balance the competing privacy interests of the individual who seeks to see his records against those of the supplier of the information who has written a frank evaluation with the expectation of confidentiality. *Id.* at 1207.

146. *See* pt. IV(A) *supra.*

147. 5 U.S.C. § 552a(e)(5)-(6).

make a reasonable attempt to insure that the record is accurate and complete.[148] There are four extremely broad exceptions to this consent prerequisite. These are: disclosure 1) to officers and employees of the agency who need the information in the performance of their duties;[149] 2) under the FOIA;[150] 3) for "routine use";[151] and 4) for law enforcement purposes.[152] Each agency must maintain an accurate accounting of the data, nature, and purpose of each record's disclosure[153] for at least five years after disclosure or for the life of the record, whichever is longer.[154] The accounting must include each recipient's name and address.[155] Upon request, the subject must have this record of accounting made available to him.[156]

The Privacy Act provides for criminal penalties where: 1) an officer or employee of the agency willfully disclosed individually identifiable information to someone who is not a proper recipient;[157] 2) an officer or employee of the agency maintains a system of records in contravention to the notice requirements of the statute;[158] and 3) any person requests or obtains any record under false pretenses knowingly and willfully.[159] In addition to criminal sanctions against individual offenders,[160] the Act establishes liability of the United States where an agency is found to have acted "willfully

148. *Id.* § 552a(b).

149. *Id.* § 552a(b)(1).

150. *Id.* § 552a(b)(2). For a discussion of the interplay between the FOIA and the Privacy Act, *see* text accompanying notes 102-05 *supra.*

151. 5 U.S.C. § 552a(b)(3) (1976). The term "routine use" is defined in the Act as "the use of such record for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7). The courts tend to leave the agencies with the discretion of determining what the term "routine use" means in the context of that agency. *See* American Federation of Government Employees (AFGE) v. Defense General Supply Center, 423 F. Supp. 481 (E.D. Va. 1976), *aff'd* 573 F.2d 184 (4th Cir. 1978).

152. 5 U.S.C. § 552a(b)(7). For a discussion of the severe and repeated repercussions of disclosure of law enforcement data contained in drug abuse data banks, *see* SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 93D CONG., 2D SESS., DRUG ABUSE DATA BANKS: CASE STUDIES IN THE PROTECTION OF PRIVACY (1974).

153. 5 U.S.C. § 552a(c)(1)(A) (1976).

154. *Id.* § 552a(c)(2).

155. *Id.* § 552a(c)(1)(B).

156. *Id.* § 552a(d)(1).

157. *Id.* § 552a(i)(1).

158. *Id.* § 552a(i)(2).

159. *Id.* § 552a(i)(3).

160. The offending party is charged with a misdemeanor and fined up to a maximum of $5,000. *Id.* § 552a(i)(1).

or intentionally."[161]

The Privacy Act of 1974 created the Privacy Protection Study Commission (the Commission)[162] to investigate the personal data recordkeeping practices of governmental and private organizations and to recommend to the President and Congress the extent to which the Privacy Act of 1974 should be applied to these organizations. After two years of study, the Commission concluded that, although the 1974 Act is a large step forward,[163] it has been unable to achieve all of its most significant goals.[164] The individual was not afforded, within reason, sufficiently extensive access to his records.[165] The Commission recommended that the ambiguous language found in the Act be clarified to harmonize variations of interpretation.[166] The Commission also suggested an amendment to the Act requiring that the record, when disclosed to the subject individual, reflect as closely as possible the form and use of the record as found within the agency[167] and that an agency supply information from "derivative records."[168] The Commission argued that these changes were necessary to enable the individual to exercise his right to correct, amend, or dispute a record once he has gained access to it.[169]

The Commission also found a need to regulate the procedures governing access to information by third parties. It was suggested

161. *Id.* § 552a(g)(4)(A) - (B). The United States is liable to the plaintiff either for the actual damages sustained or $1,000, whichever is greater, plus reasonable costs and attorney fees. *Id.*

162. Privacy Act of 1974, Pub. L. No. 93-579, § 5, 88 Stat. 1905(b)(1), as amended by Pub. L. No. 95-38, 91 Stat. 179 (1977).

163. THE PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY, 502 (1977) [hereinafter cited as PERSONAL PRIVACY].

164. *Id.*

165. *Id.*

166. *Id.* at 502-06. Some of the changes the Commission recommends include redefining "record" to include attributes and other personal characteristics assigned to an individual; adding the term "accessible record" to delineate those individually indentifiable records that ought to be available to an individual in response to an access request. *Id.* at 504.

167. *Id.* app. 4, at 121 (assessing the Privacy Act of 1974). The Commission feels that this requirement would assist an individual in determining the manner in which to exercise his right to correct, amend, or dispute a record to which he gains access. *Id.*

168. A "derivative record" is a substantially similar or derivative version tht falls within the definition of an "accessible record." There may be two kinds of derivative records: (1) exact duplicates of the original record maintained in another part of the agency; and (2) some portion of the original which has been copied and subsequently amended or merged with other records. *Id.* at 122.

169. *Id.* at 121.

that the agency be required to keep an accounting of disclosures of the subject's record both within the agency and by outside parties.[170] Records could be used internally only for the purpose for which they were originally collected;[171] external disclosures would have to be certified by an agency official responsible for overseeing the Act's implementation.[172] The Commission also recommended that the collection and maintenance of records by an agency be performed only when authorized by statute[173] and that as much information as is practical be collected from the subject individual.[174] An individual should be allowed, if possible, to decide without coercion whether to disclose the information.[175] In the event a correction of the record is received, such information would be forwarded both to sources that supplied erroneous information and prior recipients.[176]

The final report of the Privacy Protection Study Commission was transmitted to President Carter, Vice-President Mondale and House Speaker Thomas P. O'Neill on July 12, 1977.[177] The proposed privacy legislation (discussed in part IV) is based on the Commission study. The proposals attempt to resolve the Privacy Act's deficiencies by utilizing the Commission's suggestions as well as making further additions.

V. Present Legislative Proposals: Privacy Protection Within an Information-Oriented Society

A. The Privacy of Research Records Act

The Privacy of Research Records Act,[178] proposed as an amendment to the Privacy Act of 1974,[179] is designed to provide those in-

170. *Id.* at 122.

171. *Id.* at 125. *I.e.*, use of the record must fit within the routine use definition as revised. *See* note 151 *infra*, for the Privacy Act of 1974 definition of routine use.

172. PERSONAL PRIVACY, *supra* note 163, app. 4, at 125.

173. *Id.*

174. *Id.* at 126.

175. *Id.*

176. *Id.* at 127-28. It is the Commission's opinion that placing the responsibility for making corrections on the agency keeping the records is appropriate because there is no other way for the individual to safeguard against the spread of incorrect information about himself among federal government agencies. *Id.* at 128.

177. PERSONAL PRIVACY, *supra* note 163, at III-VII (introductory letters).

178. S. 867, *supra* note 16. This bill was introduced by Senator Ribicoff on April 4, 1979 and has been referred to the Committee on Governmental Affairs.

179. *See* pt. IV(b) *supra*.

dividuals who are the subjects of federally funded research with necessary privacy safeguards.[180] Seeking to invalidate many of the current policies of government agencies, the Act mandates that aggregate research results be published in such a form as to make it difficult to associate the subject individual with the statistical data.[181] It is clear that statistical studies undertaken for research purposes by their nature pose a less significant threat to the right of privacy than systems established specifically to collect data on individuals. Therefore, this proposed bill defines the term "record" very narrowly to include data which is related or traceable to individual subjects.[182]

Intimate information may be published with the consent of certain named parties[183] as long as the consent is freely given and is not compensated for in any way.[184] Without consent, such information may be published only in a medical emergency,[185] or under a judicial order issued with the intent to aid in the investigation of a transgression of the law by either the person or the agency that has conducted the research.[186] Notwithstanding these two exceptions,

---

180. S. 867, *supra* note 16, § b.

181. Such de-personalization of information is accomplished by storing the information as percentage statistics. That this solution does not impede the utilization of the research has been demonstrated by the Supreme Court's holding in Department of the Air Force v. Rose, 425 U.S. 353 (1976). For a discussion of this case *see* note 126 *supra* and accompanying text.

182. A "record" means:

(A) normal directory information;

(B) numbers, symbols, fingerprints, voiceprints, photographs, or any identifying particulars associated with an individual;

(C) information relating to an individual's background, education, finances, health, criminal or employment history;

(D) any other attributes or affiliations associated with the individual.

S. 867, *supra* note 16, § 552c(a)(1).

183. The consent of the following parties is deemed adequate:

(A) the subject individual;

(B) the parent or guardian of a subject under twelve years of age or of one who has been declared an incompetent by a court of competent jurisdiction;

(C) the administrator, executor, or trustee of a decedent's estate;

(D) a decedent's heir or next of kin.

Id. § 552c(b)(1).

184. *Id.*

185. *Id.* § 552c(b)(2)(A). However, the person must be notified within a reasonable time after the disclosure. *Id.*

186. *Id.* § 552c(b)(2)(B). Information obtained under this latter exception may be used only against the agency that has maintained the record and not against the person who is the record subject. *Id.* § (b)(2)(B)(i).

individual identity may not be disclosed unless identity is crucial in proving the violations[187] and the subject has been apprised of the intended disclosure beforehand.[188] Information may be released to statutorily authorized research auditors who, like the Federal Information Practices Board,[189] are absolutely forbidden from further disclosure of the data.[190] The research agency may contact the subject individuals only if it is necessary to accomplish the research purpose more fully and in such a manner "that minimizes the risk of harm, embarrassment, or other adverse consequences to the individual."[191] For example, in *Rural Housing Alliance v. United States Department of Agriculture,*[192] information about recipients of government housing assistance which contained data about individuals' marital status, legitimacy of children, medical histories and similarly intimate information had been collected by the Department of Agriculture as part of a study of discriminatory housing practices. The plaintiff, the Rural Housing Alliance, a private organization, contended that racial and national origin contributed to discrimination in arranging government loans for housing, and sought a copy of the report. Upon denial of such by the government, it brought suit to compel disclosure. The Court of Appeals for the District of Columbia, reversing the district court's order of disclosure, remanded the case for a reevaluation of the threat to the privacy interests of the study's subjects.[193] Holding that the plaintiff did have a legitimate interest in obtaining the information, the court nonetheless concluded that to open the private lives of the study subjects to additional scrutiny would unduly violate their expectations of confidentiality and would expose the individuals to embarrassment or possible reprisals.[194] The court recommended that alternative sources for the same information be explored and that the possibility of the Rural Housing Alliance independently asking the individuals for the same information be

187. *Id.* § 552c(b)(2)(B)(ii).

188. *Id.* § 552c(b)(2).

189. *See* pt. V(B) *infra.*

190. *See* note 222 *infra.*

191. S. 867, *supra* note 16, § 552c(b)(2)(C)(iii).

192. 498 F.2d 73 (D.C. Cir.), *supplemented,* 511 F.2d 1347 (D.C. Cir. 1974).

193. "[T]he . . . order as framed would permit release of intimate details concerning persons who could be readily identified by those familiar with the situation. . . ." *Id.* at 76.

194. *Id.*

considered.[195] The proposed Privacy of Research Records Act would codify this holding.

Despite a determination that a research purpose would be accomplished more fully with disclosure of the record, the agency that maintains the records, prior to disclosure, must conduct the classic privacy balancing test of weighing the harm that disclosure might inflict on the individual against the exigency for full exposure of the information. The justification for disclosure must clearly warrant the risk.[196] The recipient of such confidential information must protect against any further dissemination by utilizing "reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of research records,"[197] and by destroying the identifying data once need for it ceases. The recipient of such information must also sign an affidavit promising to follow these regulations.[198] The compiler of the data has the obligation, at or before collection, to give the subject individual notice if there is a possibility that such information might be further disclosed.[199] Recontact with the subject individual is prohibited absent special approval,[200] and then only after stringent precautions are taken to minimize risk or embarrassment, unless protraction would cause imminent danger to private or public health.[201] However, even emergency contact must be made in such a manner as to protect the privacy of the individual.[202] None of the research data may be used against the subject without his consent.[203] Any violations of this act are punishable by both criminal penalties[204] and civil damage judgments against the offending individual or agency.[205]

---

195. *Id.* at 78.

196. S. 867, *supra* note 16, § 552c(b)(2)(D)(ii).

197. *Id.* § 552c(iii)(I).

198. *Id.* § 552c(iv). If the recipient of information from a collector of data breaches this signed agreement, he is punishable by a fine of up to $50,000. *Id.* § 552c(j).

199. *Id.* § 552c(c).

200. *Id.* § 552c(d)(3) & (4). The approval must come from either the person or agency that most recently collected any of the information in the record directly from the individual or an institutional review board or comparable organization prescribed by the agency. *Id.* § 552c(d)(2).

201. *Id.* § 552c(d)(4).

202. *Id.*

203. *Id.* § 552c(e)(1). The consent must be in writing. *Id.*

204. "Any person who knowingly discloses information in violation of this section shall be guilty of a misdemeanor and subject to a fine of not more than $5,000 in the case of a first offense and not more than $20,000 in the case of each subsequent offense." *Id.* § 552c(h).

205. *Id.* § 552c(i). The damages recoverable may be actual damages, general damages,

Doe v. McMillan,[206] decided before the enactment of the Privacy Act of 1974, is illustrative of the type of conduct which would be governed by the Privacy of Research Records Act. In this case, a suit was brought against members of the House of Representatives, the District of Columbia School Board, the principal of the school involved and a myriad of other defendants. The plaintiffs were parents of children who attended a school which was the subject of a highly derogatory report. Throughout this report, problems concerning specifically named students were discussed. Plaintiffs requested an injunction and compensatory damages.[207] The parents alleged that the disclosure was a violation of statutory, constitutional, and common law rights to privacy and was damaging to the future reputation and good names of the children.[208] The defendants answered that the disclosure was made pursuant to its mandate to keep the public informed. Additionally, the defendants asserted that governmental immunity prevented prosecution and barred liability.[209] The Court rejected defendants' immunity claim. However, because it was uncertain whether the stated function of Congress would be seriously undermined by nondisclosure of the individuals' identities, the Court remanded the case for a determination of whether such disclosure was outside the sphere of legitimate legislative activity.[210]

---

and any equitable relief deemed proper. *Id.* It is interesting to note that this type of damage recovery had already been delineated by Warren and Brandeis as early as 1890. Warren & Brandeis, *supra* note 2, at 213.

206. 412 U.S. 306 (1972).

207. *Id.* at 309-10.

208. The most interesting part of their damage claim was that the District of Columbia School Board establish rules and regulations regarding the right of privacy of the children of the District of Columbia. *Id.* at 310 n.3. *See also* Wisconsin v. Constantineau, 400 U.S. 433, 437 (1971), where the Court advised caution "[w]here a person's good name, reputation, honor or integrity is at stake because of what the government is doing to him."

209. 412 U.S. at 317. To hold otherwise, the defendants contended, would cause Congress to be fearful of properly executing its duties. *Id.*

210. *Id.* at 324. Douglas, in his concurring opinion, concluded that the privacy balance weighed more heavily in favor of the subjects and that the functions of the report would have served equally well if the students had remained anonymous.

> We all should be painfully aware of the potentially devastating effects of congressional accusations. There are great stakes involved when officials condemn individuals by name. The age of technology has produced data banks into which all social security numbers go; and following those numbers go data in designated categories concerning the lives of members of our communities. Arrests go in, though many arrests are unconstitutional . . . . [A]lleged misdeeds or indiscretions may be devastating to a

The Privacy of Research Records Act codifies the Court's decision in *McMillan*. The nondisclosure of personal identifying information does not detract from the usefulness of statistical data, whereas disclosure of such information would constitute a serious invasion of privacy interests.

B. Federal Information and Privacy Board Act of 1978

The Federal Information and Privacy Board Act of 1978[211] proposes to establish a five-member board[212] to serve as a monitoring body for all potential infringements of privacy rights. The responsibilities of the Board would be:[213] 1) to continually oversee the general effect that information and data collection have on individual privacy;[214] 2) to investigate and assist agencies to comply with the laws[215] and policies concerned with information dissemination;[216] 3) to assist agencies in developing rules to comply with privacy laws and establish model privacy retention procedures;[217] 4) to aid those

---

person.

Id. at 329-30.

211. H.R. 350, *supra* note 17. The Federal Information and Privacy Board Act of 1978 was introduced by Rep. Barry Goldwater, Jr., in the House of Representatives on January 15, 1979 and has been referred to the Committee on Government Operations. Unlike the Privacy of Research Records Act, which sets up guidelines to be followed only by research collecting institutions, this Act seeks to establish a general information overseeing agency. *See* pt. V(A) *supra* for a discussion of the Privacy of Research Records Act.

212. The members are to be appointed by the President with the Senate's approval and will include persons knowledgeable in law, civil rights and liberties, business, records management, computer technology, communications technology, law enforcement, and information security. H.R. 350, *supra* note 17, § 2(b).

213. *Id.* § 3(a).

214. *Id.* § 3(a)(1).

215. *Id.* § 3(a)(2). The list of laws which are able to be complied with includes but is not limited to:

(A) the FOIA;
(B) the Privacy Act of 1974;
(C) the Government in the Sunshine Act;
(D) the Fair Credit Reporting Act;
(E) the Fair Credit Billing Act;
(F) the Family Educational Rights and Privacy Act of 1974.

Id.

216. *Id.* § 3(a)(3). Such information practices include:

(A) transnational data flows;
(B) electronic funds transfer;
(C) criminal history information;
(D) collection, maintenance, and use of census information.

Id.

217. *Id.* § 3(a)(4)-(5).

individuals who complain of a violation of the law;[218] 5) to report annually to the President and Congress on its activities and make recommendations;[219] and 6) to submit to the subject agency, the President, and Congress the results of any investigation it undertakes.[220] The Board would be given the authority to hold hearings and take sworn testimony and would be accorded privileges equal to any other governmental entity.[221] It would be granted unlimited access to all information that any government agency possesses, but would be prohibited from disclosing this information to third parties.[222] In this way, the Act prevents the unintentional establishment of an organization resembling the National Data Center.[223] Any information that is published in one of its reports must be devoid of all data which might directly or indirectly implicate the individual subject of the information.[224]

C. The Omnibus Right to Privacy Act

The Omnibus Right to Privacy Act of 1979,[225] which states as its purpose the protection of the privacy of individuals from both governmental and nongovernmental intrusion, is the most comprehensive of all of the privacy proposals made to date.[226] It encompasses the entire privacy scheme presented above and incorporates the en-

---

218. *Id.* § 3(a)(6).

219. *Id.* § 3(a)(8).

220. *Id.* § 3(a)(9).

221. *Id.* § 3(b). This includes the use of the mails and administrative support services. *Id.* §§ 3(b)(4)-(5).

222. *Id.* § 4(a)(1).

223. The advantages and drawbacks of a NDC have already been discussed. *See* pt. II *supra.*

224. H.R. 350, *supra* note 17, § 4(b)(1)(B).

225. H.R. 2465 was introduced before the House of Representatives on February 27, 1979 by Rep. Preyer, for himself and Rep. Goldwater. Currently, it is moving within the Government Operations Committee. Alan R. Severson, the legislative director for Rep. Goldwater, has stated that the hearings on this bill will be taking place sometime in early February. It is possible that the bill will be passed as a whole although it is more likely that only certain sections will be accepted and others rejected. In addition, it may be that S. 867, *supra* note 16 (the Privacy of Research Records Act), and H.R. 350, *supra* note 17 (the Federal Information and Privacy Board Act), will be combined with this Act. The result may be one all-encompassing act which will deal with the privacy issues raised in each. Interview with Alan R. Severson, Legislative Director, Office of Rep. Barry Goldwater, Jr., Washington, D.C. (Oct. 26, 1979) [hereinafter cited as Interview].

226. For a discussion of the Privacy of Research Records Act and the Federal Information and Practices Board Act, *see* pts. V(A) & (B) *supra.*

tire tests of certain pre-existing proposals.[227] The Act is divided into eight titles which individually address important specific aspects of privacy law. These titles are preceded by an introduction delineating the findings and purposes of the Act.[228]

In its introduction, the Act recognizes: 1) that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States";[229] 2) the need for balancing the free flow of information essential to a democratic society against the protection of personal privacy rights;[230] 3) the increasing accumulation of extensive amounts of private information by various government agencies;[231] 4) that the collection, maintenance, use and dissemination of such information has a direct effect on individual privacy;[232] 5) that more information is used and disseminated by agencies which have had no direct dealings with the individual;[233] 6) that an individual has the right to control personal information about himself;[234] 7) that the misuse of information may hamper an individual's employment, credit and other societal benefits;[235] and 8) that presently, neither law nor technology provide the individual with adequate record safeguards.[236] As a result of these findings, the Act enunciates its purposes as the following: 1) to balance what an individual must reveal to recordkeepers against what the individual seeks to gain;[237] 2) to reveal recordkeeping operations;[238] and 3) to delineate obligations as the *quid pro quo* for the use and disclosure of private information.[239]

Because the Act is a comprehensive coverage of all facets of privacy infringement, its titles deal with both private and govern-

227. One such proposal is the Federal Information and Practices Board Act. *See* pt. V(B) *supra*.

228. H.R. 2465, *supra* note 18, § 2(a) & (b). These findings are similar to those of the SUBCOMMITTEE STUDY, *supra* note 14, and the LINOWES SURVEY, *supra* note 14. In fact, much of Linowes' research has been the groundwork for the drafting of this Bill. *See* pt. III *supra*.

229. H.R. 2465, *supra* note 18, § 2(a)(1).

230. *Id.* § 2(a)(2).

231. *Id.* § 2(a)(3).

232. *Id.* § 2(a)(4).

233. *Id.* § 2(a)(5).

234. *Id.* § 2(a)(6).

235. *Id.* § 2(a)(7).

236. *Id.* § 2(a)(8).

237. *Id.* § 2(b)(1).

238. *Id.* § 2(b)(2).

239. *Id.* § 2(b)(3).

ment-initiated collection and maintenance of information. The former will be dealt with only briefly.

1. *Title I: Federal Information and Privacy Board Act of 1979*[240]

Title I is a *per verba* incorporation of the Federal Information and Privacy Board Act of 1978.[241] As discussed above, this title seeks to establish a Board as an overseer and enforcer of privacy safeguards of data collection in both the governmental and nongovernmental sectors.[242]

2. *Title II: Privacy Act Amendments of 1979*[243]

The introductory section of this Act defines terms to be used throughout the Act. Although some of the terms appear within the original Privacy Act of 1974,[244] this Act provides both additional terms and expands on included terms,[245] consistent with the recommendations of the Privacy Protection Study Commission.[246] The Act establishes guidelines for the solicitation, collection, maintenance, correction and disclosure of personal information[247] to insure that an individual can make an informed and uncoerced decision to disclose the requested information. The Act requires that a putative subject be supplied with certain information delineating the privacy safeguards which the agency is guaranteeing prior to disclosure.[248] As a limitation on the agency's powers of collection and in

240. *Id.* § 101-06.

241. *See* pt. V(B) *supra.*

242. *Id. See* note 225 *supra.*

243. H.R. 2465, *supra* note 18, § 201. Although in purpose this is identical to S. 867, *supra* note 16, their execution would differ, *i.e.*, where S. 867 seeks to add a new section, § 552c, this Act amends the existent § 552a, which is the Privacy Act of 1974 itself.

244. *See* pt. IV(B) *supra.*

245. The additional terms include: individually identifiable record; accessible record; system; subsystem; routine use; collateral. H.R. 2465, *supra* note 18, § 202(a).

246. *See* note 166 *supra* and accompanying text.

247. The last section of the proposal prohibits any federal action, until a specific statute is drafted to the contrary, that would promote the development of a standard universal personnel identifier or central population register, *i.e.*, something akin to the NDC is rejected again. H.R. 2465, *supra* note 18, § 202(c). For a definition of the universal personnel identifier *see* note 45 *supra.*

248. The information which each agency must make available to the individual includes: (i) the authority for solicitation of the information; (ii) whether disclosure is mandatory or voluntary and the consequences of not providing the information; (iii) the principal purpose for which the information will be used; (iv) any routine or collateral uses which could be reasonably expected to flow from disclosure; (v) additional information that may be used to verify that disclosed; (vi) the title, business address, and telephone number of the

order to eliminate the random and unnecessary collection of sensitive data, the Act allows the compilation of only those records that are relevant to accomplishing a purpose of the agency which a statute or presidential order authorizes.[249] The Act, however, does not prohibit agencies from collecting or maintaining information that is either expressly authorized by the subject individual or serves a reasonable and proper reference function.[250] In addition, each agency has the duty 1) to maintain accurate records in order to assure fair determinations as to the individual about whom the records are maintained;[251] 2) to assure confidentiality and security by establishing adequate administrative, technical, and physical safeguards;[252] and 3) to give subject individuals notice of disclosure under compulsory legal process.[253] No agency may collect or maintain information that in any way describes an expression by an individual in the exercise of his first amendment rights[254] unless it is in the course of an authorized investigation into illegal activities.[255]

Every federal agency is responsible for verifying the accuracy of the records maintained by both prior sources and subsequent recipients. This requires an affirmative duty to notify such sources and

---

agency official who will answer any questions the individual may have; and (vii) when information is collected for a research or statistical purpose, the possibility of it being disclosed in individually identifiable form. If disclosure is made for any other purpose, the individual must be informed that he will be promptly notified of such disclosure. H.R. 2465, *supra* note 18, § 202(k)(3)(A).

249. *Id.* § 202(e)(1)(C). *See* note 64 *supra,* for an example of a statutorily authorized purpose. As found by the Subcommittee, more than eighteen percent of the agencies collect information without any statutory authority while only sixteen percent use express statutory authority. SUBCOMMITTEE STUDY, *supra* note 14, table 3.

250. For example, a library, bibliographic or abstracting use. H.R. 2465, *supra* note 18, § 202(e)(2)(D)(ii).

251. *Id.* § 202(e)(1)(D). The Central Intelligence Agency or other criminal enforcement agencies, as exceptions, keep unverified information but must identify it clearly to users or recipients as such. *Id.*

252. *Id.* § 202(e)(1)(E).

253. *Id.* § 202(e)(1)(F).

254. *Id.* § 202(e)(2)(A). *I.e.,* the content of any public publications, speech, or other expression of belief or argument. *Id.*

255. *Id.* § 202(e)(2)(B). Thus, the stationing of undercover police officers in classrooms where meetings of university-sponsored organizations were conducted was held to be a violation of first amendent rights and the right to privacy. Gathering information for intelligence reports that did not pertain to illegal activity was permanently enjoined due to the lack of a compelling state interest. White v. Davis, 13 Cal. 3d 757, 533 P.2d 222, 120 Cal. Rptr. 94 (1975). *See also* Comment, *Police Surveillance of Political Dissidents,* 4 COL. HUMAN RIGHTS L. REV. 101 (1972).

recipients of all corrections to, or statements of disagreements with, the individually identifiable records.[256] An exception to this notification requirement is where one received the information in accordance with the FOIA.[257]

Research and statistical records kept by an agency are barred from disclosure in identifiable form with four exceptions: 1) the agency reasonably believes that disclosure will prevent imminent physical injury to an individual, "provided that the information disclosed is limited to that information necessary to secure the protection of the individual who may be injured;"[258] 2) a judicial order commands the release of such record to aid an inquiry into a violation of law, as long as the information obtained is used as evidence only against the agency maintaining the research. The information can only be disclosed in such form as to bar disclosure of the subject individual, unless such is necessary to prove the violation and the individual is given prior notice and the opportunity to contest its disclosure;[259] 3) the purpose of the disclosure is to conduct a statutorily authorized audit of the research program;[260] or 4) disclosure to the National Archives and Records Service.[261]

Agencies that maintain individually identifiable records are required to make an annual disclosure of the systems maintained, the manner in which they are used, authority for maintenance of the system, the types of individuals about whom records are maintained, each use and disclosure, and agency policies regarding access security and individual amendment of personal records.[262] One official is to be designated to oversee the proper implementation of this Act by personnel within each agency.[263]

An aggrieved subject individual may bring a civil action for breach of the requirements of this Act against the offending agency

256. H.R. 2465, *supra* note 18, § 202(f)(1).

257. *Id.* § 202(f)(2)(A).

258. *Id.* § 202(g)(1)(A). This same requirement is contained within the Privacy of Research Records Act. *See* pt. V(A) *supra.*

259. H.R. 2465, *supra* note 18, § 202(g)(1)(B)(i)-(iii).

260. *Id.* § 202(g)(1)(C).

261. *Id.* § 202(g)(1)(D). Similar provisions are contained in S. 867, *supra* note 16.

262. This detailed information is to be published in the Federal Register. H.R. 2465, *supra* note 18, § 202(h)(1)(A)-(I).

263. Such designated official is to issue standards for implementation of this section and to take reasonable affirmative steps to see to it that all agency employees are aware of the requirements of this section. *Id.* § 202(j)(1)(A)-(C).

in a district court of competent jurisdiction. The court may order any or all of the following remedies:[264] 1) an award of reasonable attorney fees and litigation costs;[265] 2) a mandate to the agency to correct the individual's records;[266] 3) an injunction against the agency to refrain from withholding the records and to make an accounting of all uses and disclosures of the particular record;[267] and 4) where the conduct of the agency is found to be intentional or willful, the award of special and general damages, not less than $1,000 or more than $10,000, to be assessed against the United States.[268] The action must be brought within either two years of the misrepresentation or two years of its discovery.[269] In addition, an official or employee of the agency or a recipient of the information who has willfully and knowingly disclosed information to one who is unauthorized to receive it is subject to misdemeanor charges.[270] Any independent contractor who performs an authorized function of the federal agency is treated as its agent; the agency could therefore, as principal, be held criminally liable for the infraction.[271] Civil liability would, in such case, rest with the contractor.[272]

Under the proposed Act, any proposal by an agency to either expand an extant system[273] or establish a new one must first be cleared by Congress and the Office of Management and Budget after it is evaluated in terms of its potential impact on privacy.[274] The President would be required to submit an annual, consolidated report to Congress, setting forth the number of records contained in each federal agency's system.[275] Where this proposed section con-

264. *Id.* § 202(k).
265. *Id.* § 202(k)(2)(B).
266. *Id.* § 202(k)(2)(A).
267. *Id.* § 202(k)(3)(A).
268. *Id.* § 202(k)(4)(A).
269. *Id.* § 202(k)(5).
270. *Id.* § 202(l)(1).
271. *Id.* § 202(m).
272. *Id.* § 202(m)(3)(B).
273. The term "system" or "subsystem" means any collection or grouping of individually identifiable records which is systematically filed, stored, or otherwise maintained according to some established retrieval scheme or indexing structure and which is, in practice, accessed by use of, or reference to, such retrieval scheme or indexing structure for the principal purpose of retrieving the records, or any portion thereof, on the basis of the identity of, or so as to identify, an individual or individuals.
Id. § 202(a)(7).
274. *Id.* § 202(o).
275. *Id.* § 202(p).

flicts with the FOIA, the Act establishes that the FOIA will control, but only to the extent that it expands the subject's access to his own record.[276] No exemption of the FOIA may be used to make inaccessible something which this proposed section makes accessible.[277]

3. *Title III: Protection of Personal Records Act*

The Protection of Personal Records Act[278] delineates the procedures to be used for disclosure of personal records by a third party recordkeeper to a federal officer, employee, or agent.[279] Such information must be obtained within the guidelines of the Fair Credit Reporting Act[280] unless the recordkeeper suspects a violation of criminal law by the subject individual.[281] Disclosure is permitted only if:[282] 1) the subject individual authorizes the disclosure of specific information in a dated and signed writing;[283] 2) an accurate accounting has been kept by the third party of all disclosures;[284] 3) the individual is given the option to revoke disclosure authorization at any time and obtain a record of disclosures theretofore made;[285] and 4) the third party does not require disclosure as a precondition of doing business with the individual.[286] The information may also be disclosed to a federal agent under the authorization of either an administrative[287] or judicial[288] subpoena, in which case there must be reasonable cause to believe that the person about whom the re-

276. *Id.* § 202(q).

277. *Id.* § 202(q)(2). For a discussion of the interaction between the FOIA and the Privacy Act of 1974 *see* Note, *An Introduction to the Federal Privacy Act of 1974 and Its Effect on the Freedom of Information Act*, 11 NEW ENGL. L. REV. 463 (1976).

278. *Id.* §§ 301-317.

279. Upon inquiry by a federal employee, private companies will disclose personal records kept in their files, regardless of the information's relevance to the agency's function. For a more detailed discussion of this issue, *see* notes 71-73 *supra* and accompanying text.

280. 15 U.S.C. § 1681b(3)(A) & (C) (1976). For a discussion of the Fair Credit Reporting Act, *see* Geltzer, *Current Practice Under the Fair Credit Reporting Act*, 65 ILL. B. J. 702 (1977) [hereinafter cited as Geltzer].

281. H.R. 2465, *supra* note 18, § 302(b)(2).

282. The Protection of Personal Records Act disclosure provisions reflect suggestions made in LINOWES SURVEY, *supra* note 14, at 9.

283. H.R. 2465, *supra* note 18, § 303(b).

284. *Id.* § 303(c).

285. *Id.* § 303(d).

286. *Id.* § 303(e).

287. *Id.* § 304(a).

288. *Id.* § 306(a).

cord is kept has violated a federal law. The evidence obtained may be used to prove only this suspected violation and not a collateral crime which might emerge.[289] Prior to subpoena disclosure, the subject individual must be served with both a copy of the subpoena and a notice which allows the subject to object to the anticipated disclosure within nineteen days of the receipt of these papers.[290] Silence on the part of the individual amounts to acquiescence.[291] Both the subject of the record and the recordkeeper have standing to challenge the subpoena's enforcement.[292] Either a search warrant issued pursuant to the Federal Rules of Criminal Procedure[293] or a grand jury subpoena to be used for the sole purpose of returning an indictment[294] may command disclosure. Information obtained that is identifiable with a particular person may be used solely for the purpose for which it is disclosed.[295] The statute of limitations for enforcing any provision of this Act is three years from the date of the violation or from its discovery, whichever is later.[296]

In a suit against either the recordkeeper or the federal agent for violation of this Act, the subject may recover: 1) actual damages; 2) general damages of not less than $1,000 nor more than $10,000; 3) punitive damages for a willful disclosure; 4) attorney fees and litigation costs; and 5) any appropriate injunctive relief.[297] In addition, a federal employee who knowingly obtains and willfully discloses information in violation of this Act is subject to a fine not to exceed $5,000, or imprisonment for a term of two years, or both.[298]

No records of an intimate nature[299] may be obtained, even by a subpoena or search warrant,[300] absent a compelling state interest.

---

289. *Id.* §§ 304(a), 306(a).

290. *Id.*

291. *Id.* § 304(a)(3)(B). The Act provides: "If neither you nor the organization named in the attached subpena [*sic*] objects to the requested information being made available to us, the information will be made available to us on and after the nineteenth day after the date on which this notice is mailed or delivered to you." *Id.*

292. *Id.* §§ 304(a)(4), 306(a)(4).

293. *Id.* § 305.

294. *Id.* § 308.

295. *Id.* § 308(2).

296. *Id.* § 314.

297. *Id.* § 315.

298. *Id.* § 316.

299. The Bill includes "business records of a sole proprietor or practitioner" within the meaning of "intimate records," *id.* § 307(a), indicating that the definition may be broadly construed.

300. *Id.* § 307.

Pursuant to the fifth amendment,[301] no individual may be compelled to testify as to these records in a criminal proceeding against him.[302]

4. *Title IV: Privacy of Public Assistance and Social Services Records Act of 1979*

The Privacy of Public Assistance and Social Services Records Act of 1979[303] establishes that as a condition precedent to the receipt of federal moneys under a federal public assistance and social services program, each state must provide measures to maintain the privacy of the records used to administer the programs involved.[304] A state statute which meets the requirements of this Act, and is not inconsistent with federal law, will be the sole authority for state agency disclosures.[305] Before any state's privacy statute will be given effect, it must be certified by the Department of Health and Welfare as consistent with the privacy principles set forth in this Act.[306] The requirements for the statute to merit certification include: 1) notice to the subject individual of the kinds of information it may collect and has collected about him, the purposes for which such information is used, terms of its disclosure, the subject's right to inspect and the extent to which eligibility for the program depends on his authorization to disclose;[307] 2) procedures for verification of data obtained from collateral sources, which includes contacting those sources in such a manner so as not to reveal the specific benefits sought by the subject.[308] The subject individual may be denied access to: 1) the identity of a source that has requested confidentiality;[309] 2) records which contain information about other clients as well;[310] and 3) records used in the course

301. U.S. CONST. amend. V. *See* Tehan v. Shott, 382 U.S. 406, 414 (1966). *But cf.* Barenblatt v. United States, 360 U.S. 109, 134 (1958).

302. H.R. 2465, *supra* note 18, § 307(b).

303. *Id.* §§ 401-404.

304. *Id.* § 402(a)(1)-(2). Some of the programs covered by this Act include those relating to: aid to families with dependant children; child support; medicaid; social services; the Food Stamp Act. *Id.* § 402(a)(2)(A)-(E).

305. *Id.* § 403(8)(E).

306. *Id.* § 403.

307. *Id.* § 403(2).

308. *Id.* § 403(3).

309. *Id.* § 403(4)(D).

310. *Id.* § 403(4)(E).

of an investigation of a suspected violation of law by the client.[311]

The agency must establish procedures that will maintain the accuracy of the records.[312] Where a change in the records is made according to the client's request, the change is to be reflected wherever information about the subject individual has been dispensed.[313] No information unrelated to the assistance program may be requested or maintained.[314]

5. *Title V: Privacy of Medical Records Act*

As the case law presently indicates, only a showing of a valid state interest will permit the collection and storage of highly sensitive medical data.[315] However, it has been repeatedly asserted by courts that confidentiality of such records must be preserved by legislative action rather than by case by case rulings of the courts.[316] Title V answers this requirement for guidelines on medical confidentiality issues. The Privacy of Medical Records Act[317] requires that subject individuals be given both access to and copies of their medical records, as well as an opportunity to correct erroneous entries.[318] Medical records may be disclosed only under the fol-

311. *Id.* § 403(4)(F).

312. *Id.* § 403(7).

313. *Id.* § 403(6)(A)(ii).

314. *Id.* § 403(8).

315. *See* State v. Jacobus, 75 Misc. 2d 840, 348 N.Y.S. 2d 907 (Sup. Ct. 1973). *See generally* Kaiser, *Patients' Rights of Access to their Own Medical Records: The Need for New Law*, 24 BUFFALO L. REV. 317 (1975).

316. *See, e.g.*, State v. Jacobus, 75 Misc. 2d 840, 348 N.Y.S.2d 907 (Sup. Ct. 1973), where the court held that the state could not compel doctors to record the names and addresses of parents of aborted fetuses so long as confidentiality was not safeguarded sufficiently by legislative enactment. *Id.* at 846, 348 N.Y.S.2d at 913-14. *See generally* Clement, *The Rights of Submitters to Prevent Agency Disclosure of Confidential Business Information: The Reverse Freedom of Information Lawsuit*, 55 TEX. L. REV. 587 (1977).

317. H.R. 2465, *supra* note 18, §§ 501-502. According to Alan Severson, legislative director in the office of Rep. Goldwater, this section of the bill has already been considered by Congress and will be debated further in the next session. Interview, *supra* note 225. The topic of medical disclosures, however, is beyond the scope of this Comment.

318. H.R. 2465, *supra* note 18, § 502 (amending 42 U.S.C. § 1306 (1976)) sets out the correction procedures as:

(1) thirty days after the individual's request, the medical facility must
   (a) make the correction requested and so inform the individual, or
   (b) inform the individual of the reasons for refusal to correct and the right to review.

(2) any such request for correction must accompany subsequent disclosures to other parties.

lowing conditions:[319] 1) the person requesting the information must be properly identified;[320] 2) the records may be disclosed only to the extent needed;[321] 3) no disclosure, with the exception of specified conditions,[322] may be made without the individual's authorization.[323] Compliance with this Act is a condition precedent to the facility's participation in the Medicare and Medicaid programs.[324]

6. *Title VI: Fair Credit Reporting Act Privacy Amendments*[325]

The purpose of these amendments is to require that consumer reporting agencies[326] maintain reasonable procedures to prevent dis-

---

(3) at the individual's request, prior recipients must be notified of the protestations. *Id.*

319. *Id.* In Schulman v. New York City Health & Hosp. Corp., 44 A.D. 2d 482, 355 N.Y.S.2d 781 (1974), a case addressing a similar issue, the court held that, since confidentiality of the plaintiff's abortion record was adequately insured by a requirement that these records not be subject to subpoena or to inspection by anyone other than authorized personnel of the New York City Health Department, filing of a certificate with the Health Department would not be invalidated. The records were to be disclosed only to the Department's authorized personnel and only to the extent that they be used (1) for followups in case of complications; (2) investigation of the propriety of procedures at the facility; and (3) to offer health counseling on family planning, venereal disease, and Rh factor treatment. *Id.* at 485-86, 355 N.Y.S.2d at 784-85.

320. H.R. 2465, *supra* note 18, § 502 (amending 42 U.S.C. § 1306 (1976)).

321. *Id.* § 502 (amending 42 U.S.C. § 1306 (1976)).

322. The specified conditions include:

(1) disclosure to an employee of the facility in the course of his duties;
(2) disclosure to a health professional consulted by the facility;
(3) disclosure due to compelling circumstances of health or safety;
(4) disclosure for use in a health services project;
(5) disclosure for specified Governmental audits and evaluations;
(6) disclosure to a public health authority pursuant to statute;
(7) disclosure of specified information to a law enforcement authority;
(8) disclosure which reveals only the presence of the individual at the facility for admission purposes;
(9) disclosure pursuant to an administrative or judicial subpoena.

Id.

323. *Id.*

324. *Id.*

325. 15 U.S.C. § 1681 (1976). Extensive discussion of the Fair Credit Reporting Act is beyond the scope of this Comment. It should be noted here that Rep. Cavanaugh introduced a bill before the House of Representatives on October 12, 1979, the first title of which is an amendment to the Fair Credit Reporting Act. H.R. 559, *supra* note 19. For a more detailed analysis of the Fair Credit Reporting Act, *see* Geltzer, *supra* note 280.

326. The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties,

closure of consumer information to unauthorized[327] persons and to prevent disclosure of inaccurate, highly damaging information. Consumers who are adversely affected by a credit decision must be given specific information[328] and must be allowed the opportunity to dispute the accuracy of any item contained in their dossiers.[329] This Act also sets standards to be followed by depository institutions[330] and insurance companies[331] when disclosing information possessed by them.[332] The Federal Trade Commission is granted authority to issue regulations governing the disclosure of information by these institutions and to enforce this title.[333]

7. *Title VII: Confidentiality of Tax Records Act*[334]

This Act amends the Internal Revenue Code. It restricts disclo-

---

and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f)(1976).

327. Authorized use can be defined as "whether the use of the mercantile agency is a reasonably necessary method of obtaining indispensable information." Smith, *Conditional Privilege for Mercantile Agencies* — MacIntosh v. Dun, 14 COLUM. L. REV. 187, 210 (1914).

328. The consumer must be told of the specific reason leading to the adverse decision, the specific items of information which support the reason, and the consumer's right to inspect and copy the information used by the creditor. H.R. 2465, *supra* note 18, § 602(j)(1)(a)(1)-(3).

329. *Id.*

330. *Id.* § 657(1).

331. *Id.* § 688(3).

332. *Id.* §§ 652-653, 655, 671-672, 676. Depository institutions must disclose to the consumer the types of information which may be collected and all types of institutions which may collect such information. No information which is not described in the disclosure to the consumer may be collected. Should an adverse decision be made, the consumer must be told of the specific reason for the decision, the items of information which led to such a decision, and the consumer's right to inspect all information used to arrive at the decision. If any information furnished by the institution to the consumer agency is found to be inaccurate, the institution must inform the consumer agency about the inaccuracy. *Id.* §§ 652, 653, 655.

Insurance companies must give the customer access to all information contained in his file unless the information has been compiled in the process of settling a claim. The individual may correct discrepancies which must be communicated to other recipients by the company. If there is a refusal by the insurance company to correct, the individual must be afforded the opportunity to insert his protest in his file, which will be attached to any future promulgation of the record and will be forwarded to any institution which has, in the two years prior to this protest, received such information. No insurance institution may make an adverse underwriting decision based solely on a previous adverse underwriting decision. *Id.* §§ 671, 672, 676.

333. *Id.* § 687.

334. *Id.* §§ 701-706. For a discussion of the misuse of tax data by the IRS, *see generally* WAR ON PRIVACY 220-23 (L. Sobel ed. 1976).

sure by the Internal Revenue Service and state tax officials of information contained on taxpayer returns to matters pertaining to: 1) prospective jurors;[335] 2) state tax enforcement;[336] 3) investigations of prospective federal appointees;[337] 4) enforcement of child support obligations;[338] and 5) enforcement of a specifically designated federal statute, *i.e.*, not related to tax administration.[339] The head of the interested federal agency is required to bring suit against the taxpayer to compel disclosure of the aforementioned information.[340] The district court may grant such a request only after the agency has met the burden of proving the following four requirements:[341] 1) there is probable cause to believe that a specific federal statute has been violated;[342] 2) such return information is probative evidence in determining the alleged violation;[343] 3) there is no rule of law preventing the particular disclosure;[344] and 4) after reasonable diligence, no other source was found that could yield the information

335. H.R. 2465, *supra* note 18, § 702 (repealing I.R.C. § 6103(h)(5)).

336. *Id.* § 703.

337. *Id.* § 704. Before disclosure of the appointee's return information, the individual must be notified in writing of the request for such disclosure and must express his assent in writing. *Id.*

338. *Id.* § 705(6)(B) (amending I.R.C. § 6103(l)(6)). "The Secretary shall disclose return information . . . only for purposes of, and to the extent necessary in, locating individuals owing child support obligations." *Id.*

339. *Id.* § 706(b)(1)(A) (amending I.R.C. § 6103(i)).

> Pursuant to a determination in a civil action . . . , a return or return information shall be open, but only to the extent necessary as provided in such determination, to officers and employees of a Federal agency personally and directly engaged in, and solely for their use in preparation for, any administrative or judicial proceeding (or any investigation which may result in such a proceeding) pertaining to the enforcement of a specifically designated Federal statute (not involving tax aministration [*sic*]) to which the United States or such agency is or may be a party.

Id.

340. *Id.* § 706(b)(1)(B). Senator Lowell Weicker has said: "If an agency needs to know something that is contained in a tax return, why not ask the taxpayer directly. Because the tax return makes bureaucratic investigation easier is not sufficient reason to skirt standard judicial remedies . . . ." N.Y.L.J., Oct. 7, 1974, at 4, col. 5.

341. H.R. 2465, *supra* note 18, § 706(b)(1)(B).

342. *Id.* § 706(b)(1)(B)(i).

343. *Id.* § 706(b)(1)(B)(ii). *See* Garner v. United States, 501 F.2d 228 (9th Cir. 1974), *cert. denied*, 426 U.S. 948 (1975), where the court, siting *en banc*, affirmed the gambling conviction of the defendant. The prosecution's case-in-chief was based on tax returns which reported the defendant's source of income as wagering and gambling. For a discussion of the self-incrimination problem involved, *see* Note, *The Use of Tax Returns in Non-Tax Prosecutions*, 41 BROOKLYN L. REV. 580 (1975).

344. H.R. 2465, *supra* note 18, § 706(b)(1)(B)(iii).

sought.[345] Disclosure is barred until all channels of appellate review are exhausted.[346] The agency may be held responsible for attorney fees and all costs of litigation if the taxpayer prevails.[347]

8. *Title VIII: Family Educational Rights and Privacy Amendments of 1979*[348]

This section amends the General Education Provisions Act.[349] It requires educational institutions to formulate and adopt a written policy providing protections for the privacy of personal information.[350] Such policy must provide: 1) access to student records by the students and their parents;[351] 2) restriction on access to these records by third parties;[352] 3) the right to challenge extant information and insert clarifying materials;[353] 4) a description of the types of information that may be released without the subject's consent[354] and those that do require such consent;[355] 5) a definition of the role of the students and parents in formulating the institutions' privacy policies;[356] and 6) enforcement of such policies by the institutions themselves as well as the district courts.[357] Federal funds may be withheld from the educational institution to enforce compliance with the guidelines set forth in this Act.[358] The subject individual may bring an action either to compel the

345. *Id.* § 706(b)(1)(B)(iv).

346. *Id.* § 706(b)(1)(G).

347. *Id.* § 706(b)(1)(D).

348. *Id.* §§ 801-802. Educational Privacy Rights is a very broad topic and will only be touched on in this Comment to the extent that it coincides with the federal privacy concerns. For a discussion of such issues, *see* Snyder, *Confidentiality and Student Records*, in THE RIGHT TO BE LET ALONE: PRIVACY IN THE UNITED STATES 95-113 (1976).

349. H.R. 2465, *supra* note 18, (amending 20 U.S.C. 1232g (1976)).

350. *Id.* § 802.

351. *Id.* § 802(1).

352. *Id.* § 802(2)(b)(1).

353. *Id.* § 802(6).

354. *Id.* § 802(11).

355. *Id.* § 802(12).

356. *Id.* This is one of the requests the plaintiffs made in Doe v. McMillan, 412 U.S. 306 (1972). *See* notes 207-08 *supra*, and accompanying text.

357. H.R. 2465, *supra* note 18, § 802(23).

358. *Id.* § 802(22). Funds are to be withheld if:

> (1) the policy adopted by the institution does not conform to this Act; or (2) there has been a systematic failure on the part of the institution to enforce such a policy; and (3) sufficient steps to correct this failure have not been taken by the institution after it has received notice of the infraction.

The sum withheld is to be proportionate to the nature of the violation. *Id.*

institution to grant him the right of inspection or to enjoin release of a record.[359] The institution may be compelled to pay costs of litigation.[360]

D. Review

Various solutions similar to sections of the Bill were suggested prior to the introduction of the Omnibus Bill. One writer[361] suggested self-regulation of the data systems by the computer industry within certain specified guidelines,[362] one of which includes an organization composed of representatives of the computer industry whose duty it would be to promulgate and enforce the desired standards.[363] This organization would have the power to conduct periodic inspections, conciliate disputes between customers, companies and citizens, license or certify the system in issue contingent on adequate privacy safeguards, promulgate and enforce a code of conduct for programmers and key personnel and impose sanctions on violators.[364] Another writer[365] suggested five alternative approaches, the most important of which is the establishment of a new federal agency which would fashion regulations providing for:[366] a) notice to subject individuals, b) a review board which would meet new situations as they arise, c) authorization of inspectors, d) the power to license and certify agencies on the basis of their adherence to established rules, e) bonding and insuring of personnel, and f) self-regulation.[367]

The Omnibus Right of Privacy Act seeks to balance the interests of the individual against society in three ways. First, the Bill restricts the collection of information to only that which is relevant to the agency's purposes.[368] This restriction is accomplished by requiring, within the appropriate titles, that the individual be told

359. *Id.* § 802(23).

360. *Id.* For an example of the type of situation which this Act seeks to pre-empt, *see* Doe v. McMillan, 412 U.S. 306 (1972). *See* note 206 *supra* and accompanying text.

361. Grenier, *Computers and Privacy: A Proposal for Self-Regulation*, 1970 DUKE L.J. 495. Although the suggestions contained in this article relate to infringement by private companies, they are a useful example of the general trend and view of regulation.

362. *Id.* at 505-13.

363. *Id.* at 507.

364. *Id.* at 507-08.

365. Comment, *The Computer Data Bank-Privacy Controversy Revisited: An Analysis and Administrative Proposal*, 22 CATH. U. L. REV. 628 (1973).

366. *Id.* at 643-45.

367. *Id.* at 648-49.

368. H.R. 2465, *supra* note 18, § 202(k)(3)(A).

what effect his withholding of information will have on the decision to be made in his behalf[369] and that the individual be allowed to control, in part, the extent to which identifiable information concerning him will be revealed to other agencies.[370] Second, the Bill requires that subject individuals be informed of the pertinent information maintained by federal agencies.[371] This is effected by: requiring both authorization for maintenance of data banks[372] and the disclosure to the individual of the intended uses of pertinent information;[373] affording the subject the opportunity to review his own files and to make protestations and corrections;[374] and giving the individual adequate legal and equitable remedies as compensation for a violation of his rights.[375] Finally, the Bill delineates the obligations of the agency attendant to the use and disclosure of private data.[376] The Omnibus Bill, if passed, will effectively give the agencies adequate notice of their duties and liabilities in relation to the protection of individual privacy rights of the subjects of their data banks.

VI. Conclusion

Infringement on individual privacy, as indicated by the Subcommittee's findings,[377] has become quite extensive and should not be accepted as a necessary and inevitable outgrowth of technological advancement. The protection of important, constitutionally protected rights demands that many of the proposals now before Congress be enacted as a comprehensive scheme. Such legislation will insure effective control over data collection in an area now secured by *ad hoc,* and often conflicting or unobserved, agency practices. The deficiencies in the present statutory scheme have been clearly demonstrated by the Privacy Protection Study Commission in its assessment of the Privacy Act of 1974 and the FOIA.[378] Congress has rejected the proposal of one central repository for all of the sta-

369. *Id.* § 403(2).
370. *Id.* § 303(b).
371. H.R. 2465, *supra* note 18, § 2(b)(2).
372. *Id.* § 202(h)(1)(A)-(I), (o).
373. *Id.* § 403(2).
374. *Id.* § 403(6)(A)(ii).
375. *Id.* § 202(k).
376. *Id.* § 2(b)(3).
377. *See* pt. III *supra.*
378. *See* pt. IV *supra.*

tistical information collected by the federal government because of the unresolved security problems inherent in such a system. The proposed Omnibus Bill properly balances an individual's privacy interests against society's interest in a free flow of information. By allowing the aggrieved individual a definite remedy in the case of infringement and injury,[379] the bills provide a necessary means for vindication of the individual's right of privacy. Collection and dissemination of only relevant material, and only with the consent of the subject individual who is aware of the contents of his file, serves as a further check on privacy encroachments.[380] These practices would also provide for accuracy of much information that now may be unreliable. Vesting a central body with the responsibility of monitoring federal agencies' information practices will increase the effectiveness of the individual's remedies.[381]

The outcome of the Congressional debates on the pending privacy legislation remains to be seen.[382] It is true that the objectives and principles involved are difficult to reconcile. The resulting choices are often contradictory and the scientific aspects of data collection are new and continually changing. But the right involved is not new or foreign. It is an historically recognized right to have some control over one's "inviolate personality."[383] A comprehensive national information policy is essential if this critical right of privacy is to survive in the age of technology.

Ludmila Kaniuga-Golad

379. Each Act provides for civil and criminal penalties for the subject of the information against the dissemination agency. *See, e.g.*, note 297 *supra*.

380. The Privacy of Research Records Act, for example, allows publication of intimate information only after consent is freely given, with the exception of a medical emergency or a judicial order. *See* notes 183-90 *supra* and accompanying text.

381. This is the intent of the proposed Federal Information and Privacy Board Act. *See* pt. V(B) *supra*.

382. *Id.*

383. Warren & Brandeis, *supra* note 2, at 205.